

# “The early bird catches the worm”: anticipating the challenges and opportunities of PSD2

In November 2015, the Council of the European Union took an important step toward integrating the payments market. Broadening its regulatory scope to include both traditional and emerging payment systems actors, the Revised Payment Services Directive (PSD2) creates a level playing field for all. This reflects recent developments in consumer spending trends, and provides affected stakeholders with a clear wakeup call. The payments market has shifted, consumers expect different services, and authorities are aligning their regulations accordingly. The text of the Directive creates both significant challenges and a wealth of opportunities—and it is not advisable to turn a blind eye to either. Understanding changes and reacting early will be key to yielding the best results.



## The changing relationship between consumers and payments

Now more than ever, consumers are dictating how operations should be run in a wide range of sectors, and the payments market is an excellent example of this. Reflecting the significant development of e-commerce and the deeper penetration of mobile devices in consumers' daily routines, the payments market has evolved into a space where payments can be executed without having to go through a bank. Instead, payers can pay directly via the merchant's platform using their smartphones, with transparent and easy access to their own finances. These consumer habits are predominantly led by the so-called "Generation Y": the cohort of individuals who came of age at the turn of the 21<sup>st</sup> century. This is a much more technologically savvy age group, increasingly open to new payment and purchase structures.<sup>1</sup>

This development has not gone unnoticed in the FinTech sector. We are seeing a clear increase in entities that either allow consumers to view their entire financial situation or to initiate payments themselves in an extremely user-friendly, personalised and real-time way. These consumer habits, coupled with emerging FinTech technology, represent the drivers of today's era of innovation. In order to reap the greatest benefits, efforts should be made to ensure that the entire payments market works at its optimal level for all stakeholders—consumers, merchants and Payment Services Providers (PSPs).

In the context of a disrupted payments market and different consumer expectations, the EU has designed a new directive to regulate the actions of all active members of the payments value chain. Stakeholders are now finding themselves at an important stage in the evolution of the payments system, where inaction is not an option. Instead, it is essential that they recognise the most relevant challenges and opportunities, and react accordingly.

## The EU aligns regulations to the changing landscape: PSD2

The EU plays an important role in designing regulations that are optimally tailored to changing payment trends. The payments market has been regulated since 2007 by the Payment Services Directive (PSD), which was formally replaced in December 2015 by PSD2.<sup>2</sup> This represents the EU's effort to align its regulatory framework with the reality of consumers' needs, habits and preferences as well as the rapidly evolving technologies involved.

### PSD2 brings changes in four main areas:

- range of transactions
- scope of stakeholders
- liability
- access to information and security

As a whole, its provisions are designed to increase competition, and push for payments that are more innovative, efficient, swift and secure for consumers.

In light of the growth in cross-border transactions, and the fact that they often entail higher costs and longer processing times,<sup>3</sup> the Directive extends the EU's regulatory scope to transactions in any currency where only one of the PSPs at either end is within the EU ("one-leg-out transactions"). PSD2 also creates a new category of PSP, Third-Party Service Providers (TPSPs), which includes Account Information Service Providers (AISPs) and Payment Information Service Providers (PISPs). The former offer a complete view of the payer's accounts across all relevant financial institutions, while the latter act as a bridge between the payer's and the payee's banking platforms. These players introduce significant benefits for payment users, including both consumers and merchants. On the one hand, TPSPs represent a tool for consumers and merchants to always have a full overview of their accounts, without accessing each banking platform separately. This is a significant enabler for informed payment and purchasing choices. On the other

hand, payers and payees are in direct contact with each other, without having to go through their respective banking platforms. To top it all off, all services are available virtually, without requiring payers to move any further than their mobile device (usually a mobile phone or tablet). Together, they provide consumers with a significantly improved payment and purchasing experience. In order for TPSPs to operate, banks are required to fulfil account information and payment initiation requests by providing TPSPs with the necessary information via Application Programming Interfaces (APIs)—where authorised by the payer.

Indeed, it is clear that the payer receives the most attention in the Directive: payers are provided with increased protection in case of incorrectly executed payments; payments always have to be processed on the basis of "strong customer authentication"; and any information on the payer exchanged via APIs cannot be retained beyond the purpose of completing the payment. ➔


We are seeing a clear increase in entities that either allow consumers to view their entire financial situation or to initiate payments themselves in an extremely user-friendly, personalised and realtime way.

1. Suren Ramasubbu, The Huffington Post, July 2015

2. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

3. European Central Bank, September 2010 and 1999

**Table 1 - The main PSD2 provisions by area**

	<ul style="list-style-type: none"> <li>• In terms of transparency and information provisions, regulated transactions also include those in any currency where only one of the PSPs is within the EU (“one leg-out transactions”)</li> <li>• These provisions apply to those parts of the payment chain that are carried out within the EU</li> </ul>
	<ul style="list-style-type: none"> <li>• New category of PSP: TPSPs, including AISP and PISP</li> <li>• They both have to register as payment institutions with the local regulator</li> <li>• Banks have to provide AISP and PISP with access to information on the payer’s account whenever prompted to do so by a request supported by permission from payers themselves</li> <li>• The connection between banks and TPSPs is established via APIs</li> </ul>
	<ul style="list-style-type: none"> <li>• PSPs become fully responsible for proving that payments were (or were not) correctly executed</li> <li>• PSPs are required to cover the ensuing reimbursement of the payment account, as well as any related fees, charges or interest that the payer may incur</li> <li>• Payers are only fully liable if their behavior was fraudulent or grossly negligent</li> <li>• Except for these cases, the highest fee a payer can be liable for is reduced from €150 to €50</li> <li>• PSPs should be protected against any liability with regard to the relevant bank and PSU. Both AISP and PISP are required to hold professional indemnity insurance that covers all territories in which they operate account information and payment initiation services</li> </ul>
	<ul style="list-style-type: none"> <li>• TPSPs may only access and use information on payers and their accounts for the purposes of processing the payment. Information cannot be stored, and any personalised security credentials should always be communicated among PSPs securely</li> <li>• PSPs must implement strong customer authentication in order to validate the identity of the payer, i.e., the use of at least two of three independent features including “knowledge”, “possession” and “inherence”</li> <li>• PSPs must implement an incident reporting structure in case of major operational and security incidents</li> <li>• PSPs are required to implement an appropriate risk and control management framework, performing a comprehensive assessment of the operational and security risks, to be submitted to the relevant authority at least once per year</li> </ul>

**The impact on banks: key drivers for an amended business model**

**Challenges:** once each Member State has transposed the Directive into national legislation, banks will have to comply with significant information and technology requirements—specifically with regard to setting up APIs and ensuring strong customer authentication. These obligations are at odds with the kind of infrastructure that most banks have inherited from the pre-digital era. For many, complying with PSD2 will require significant costs in relation to implementing the new IT structures. However, the severity of this may vary depending on whether a bank is already at an advanced stage with regard to strong customer authentication; such players will only need to implement an open API.

This IT cost could affect the operative costs related to the bank’s payment activity, resulting in a loss of the direct relationship with those consumers and merchants, who will instead opt for TPSPs to initiate payments and gather information on their accounts. This growing preference for disintermediated/virtual payments is fueled by banks’ inability to provide a customer experience that is as user-friendly and real-time as those offered by TPSPs. The personal, mobile, and swift nature of TPSP services is in conflict with how banks traditionally operate—i.e., one-size-fits-all products distributed on the basis of physical presence.

In complying with PSD2 requirements, banks will not only have to implement changes to IT infrastructure, but also—and just as importantly—ensure that their strategy, culture, skillset, and regulatory knowledge is properly aligned. This is particularly important given that banks will now be officially competing with other stakeholders on the same playing field, and these stakeholders are much more technologically advanced and aligned with consumer needs.

In general, banks are hindered by the lack of a clear and complete overview of national legislation. Indeed, several

**Figure 1 - Impact on banks: challenges**



PSD2 requirements have to be read in conjunction with specific rules by the European Banking Authority (EBA), which is in charge of establishing Regulatory Technical Standards (RTS) for strong customer authentication, secure communication, cooperation and exchange of information for passporting, as well as Guidelines on implementing the appropriate risk and control management framework. There is currently no industry standard in relation to the framework around APIs.

However, the majority of European Banks have already engaged in opening up dedicated test areas in their websites where they publish their APIs and developers are encouraged to build and test their own apps. At the same time, several European initiatives are underway (eg the Berlin Group, PRETA, STET), aiming to develop PSD2 API standards to allow Third Party Providers (TPSPs) to access payment accounts.

**Opportunities:** each challenge that banks face comes with an associated opportunity that, if leveraged in a timely manner, will ensure that “the early bird catches the worm.”

Banks will have to set up APIs for information to be available to AISP and PISPs. Banks should consider developing APIs by differentiating between those

services and functions that fulfil the basic requirements of PSD2, and those that go further—and which can be capitalised upon. Banks could offer these other services at a cost and based on a contract to be agreed between the bank and the TPSP. This could compensate for the cost of the IT infrastructure change, and also become a source of profit. It should be noted that any such strategy would be dependent on the RTS published by the EBA in February 2017.

When considering the trend of consumers shifting from traditional payments through banks to the disintermediation offered by TPSPs, banks should account for the advantage they still hold and are not likely to dramatically and completely lose to TPSPs: banks are endowed with far stronger brands, they still have a far broader customer audience, and they benefit from a wealth of big data on their customers. This does not mean that banks should be content to stick with the status quo. On the contrary, the best way for banks to benefit is to ensure that they are not buried under an outdated infrastructure, and concerted efforts should be made to adapt to the market’s needs and expectations, taking this opportunity to design and implement simplification and optimisation strategies. ➔

Figure 2 - Impact on banks: opportunities

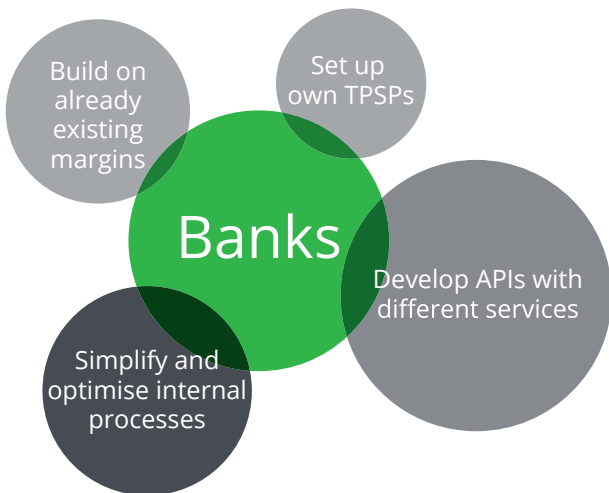
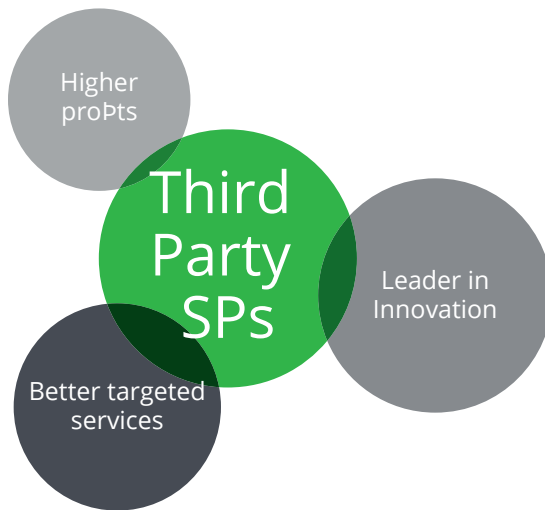


Figure 3 - Impact on TPSPs: opportunities



It is important for banks to act on this opportunity now, while they are waiting for the Central Bank of Cyprus to implement PSD2. It is a precious two-year buffer zone, during which banks should prioritise designing and integrating strategies to secure their customer audience. By refining the services on offer and their operational and IT infrastructure, they can protect or even increase their share of customers before TPSPs get there first. Improvements could include, but are not limited to, the areas of big data, analytics and cross-border transactions.

Finally, while it is true that a growing number of TPSPs are increasing the level of competition, this does not rule out the possibility for banks to set up their own TPSPs.<sup>4</sup> Under PSD2, banks are indeed eligible to provide account information and payment initiation services.<sup>5</sup> Moreover, if banks recognise and properly invest in the opportunities that have already been identified (APIs with specific monetised services, existing margins, and simplified and optimised infrastructure), the account information and payment initiation services offered by banks could become even more appealing to both consumers and merchants.

**The impact on TPSPs: ensuring the golden era is sustainable**

**Opportunities:** TPSPs and the FinTech sector in general appear as the obvious

“winners” from PSD2. And with good reason. They are presented with fertile ground for the services they offer, particularly as consumers increasingly prefer to initiate payments through TPSPs rather than directly through their banks. It is easy to see why TPSPs could escalate their profits by expanding their customer base. Moreover, their very nature and business model ties them to certain specific activities (either account information or payment initiation), meaning that they can pick and choose the segments of the audience they want to target. Unlike banks, TPSPs do not have the burden of meeting all of the needs and expectations of the entire consumer and merchant audience.

On top of this, TPSPs can improve their services by refining and better-targeting them on the basis of the information that they compile every time a customer initiates a payment or requests to view their accounts online.<sup>6</sup> As consumers remain in the driving seat setting the agenda for the payments market, TPSPs can focus on understanding how payment initiation and information request trends are evolving, to better anticipate or adjust accordingly.

Equipped with these healthy and solid capabilities and facilitated by these unique conditions, TPSPs are clearly leading the innovation race, positioning themselves way ahead of banks.

**Challenges:** in order to safeguard their advanced position in the payments market,

TPSPs do however still have to ensure that they recognise, react to, and mitigate some noteworthy challenges.

While it is true that consumer preferences are shifting, TPSPs are undeniably the new kids on the block compared to the well-established banks. Banks may have suffered a significant blow with regard to consumer trust during and after the financial crisis, but they do maintain excellently marketed brands as well as a significant history. This is ultimately reflected by their reach and, as already mentioned, banks still have the majority of what TPSPs must heavily invest in building: a customer audience. TPSPs will have to approach this by identifying the right segments to target (e.g., millennials, merchants). Indeed, the fact that they specialise in either account information or payment initiation services may play to their advantage (see above) as well as disadvantage, ruling out a lot of potential consumers who may have difficulties in understanding the services offered by these new entities.

The risk of not connecting with as many consumers as a bank already can comes in addition to the boundaries set by PSD2 regarding access to accounts. PSD2 in fact prohibits TPSPs from keeping information on the payer after the execution of the payment.<sup>7</sup> Without added, comprehensive, and detailed information on consumers, TPSPs are unable to develop any further

4. Chris Skinner, The Finanser, November 2015

5. Annex 1, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

6. Finextra, February 2016

**Figure 4 - Impact on TPSPs: challenges**

services that would allow them to target untapped consumer segments.

Access to accounts is just one example of the overarching challenges that PSD2 presents to TPSPs: while already active in the payments market, they have only just become regulated now. The regulatory burden will mean that they must cover certain aspects for the first time: these include having to register as a payment institution with the local regulator, setting up risk and control frameworks, complying with all relevant reporting obligations, and performing AML and KYC controls.

Consequently, TPSPs will have to engage a significant amount of resources and time in liaising with new stakeholders, as well as in learning about, applying and complying with the regulatory framework. This is a context that until now they did not need—or know how—to operate within.

Finally, when evaluating their competitive and advanced position, TPSPs should maintain a comprehensive overview of all players on the field. Indeed, while TPSPs seem at first glance to be competing with banks, they are also competing with each other. And the natural question arises: how many AISPs and PISPs are too many? Given that they already risk being left out of certain segments of the customer audience, they should certainly consider the possibility of the market becoming saturated with fellow

TPSPs. In this regard, monitoring how PSD2 is transposed into national laws will be crucial, specifically in terms of the requirements for the relationship between payment stakeholders. Indeed, the more standardised and harmonised the relationships, the simpler it will become for TPSPs to learn how to position themselves with regard to banks, and the easier it will be for new TPSPs to enter the market.

#### The impact on already authorised EMIs/PSPs

Based on guidance from European regulators, a number of additional requirements is likely to become applicable from already authorised EMIs and PSPs. These relate to the following areas and additional supporting information will likely have to be provided to the regulator:

- Procedures for incident reporting.
- Processes in place to file, monitor, track and restrict access to sensitive payment data.
- Principles and definitions they apply for collecting statistical data on performance, transactions and fraud.
- Arrangements for business continuity and the procedure for testing and reviewing these plans.
- Security policy, including risk assessment and mitigation measures to adequately protect payment service users against

## Making the relationship work: coopetition

In conclusion, the entry into force of PSD2 offers important opportunities. On the one hand, banks need to consider how to design their business model around payments as well as how to structure their relationship with new entrants. On the other hand, TPSPs need to come to terms with the loss of their unsupervised and unregulated status.

While these impacts are specific to the type of stakeholder, they cannot be tackled solely from the comfort of one's sofa.

Indeed, there is no escaping the fact that since PSD2 was published in the Official Journal of the European Union in December 2015, banks and TPSPs are officially operating in the same room, under common regulatory requirements, and ultimately serving the same customers. In order to make the cohabitation as mutually beneficial as possible, coopetition will be key. That is, a strategy to secure marketshare through interaction rather than struggle, and recognising that, at the end of the day, it is not likely to be a "winner takes all" situation, as both stakeholders are needed for the healthy functioning of the emerging payments ecosystem.

identified risks, including fraud and illegal use of sensitive and personal data.

- Description of checks on agents and branches.
- Professional indemnity insurance held (for firms that propose providing account information or payment initiation services).
- Security requirements for APIs

7. Articles 66-67, "Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC"

# How Deloitte can help you

Our experienced team of experts can support your organisation:

- Strategic Impact Assessment (Readiness Test)
- Gap analysis and Remediation plan
- Regulatory reporting and support
- Design and Implementation of Security and Authentication framework
- Business model redefinition
- Implementation support
- Advisory services in relation to Data Protection
- Support around designing and building your APIs

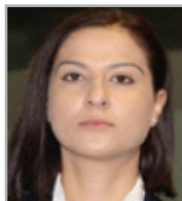
## Contacts

If you require any further information on any of the issues mentioned in this material and on how Deloitte can help you address the challenges ahead, please do not hesitate to contact



**Panicos G. Papamichael**

Partner | Risk Advisory Services Leader  
ppapamichael@deloitte.com  
Direct line: +357 22 360805



**Clea Evagorou**

Director | Risk Advisory  
clevagorou@deloitte.com  
Direct line: +357 22 360600



**Chris Antoniadis**

Manager | Risk Advisory  
cantoniades@deloitte.com  
Direct: +357 22 360622



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

Deloitte Limited is the Cyprus member firm of DTTL. Deloitte Cyprus is among the nation's leading professional services firms, providing audit, tax, consulting and financial advisory services through over 650 people in Nicosia, Limassol and Larnaca. For more information, please visit the Cyprus firm's website at [www.deloitte.com/cy](http://www.deloitte.com/cy).

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 245,000 professionals are committed to making an impact that matters.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network should be responsible for any loss whatsoever sustained by any person who relies on this communication.

Deloitte Limited is a private company registered in Cyprus (Reg. No. 162812).  
Offices: Nicosia, Limassol, Larnaca.