

The Second Payment Services Directive (PSD2)

The payment industry landscape is changing

WHAT IS PSD2?

When the first Payment Services Directive (PSD) was introduced in 2007, it was done with the intention of creating a single payments landscape across the European Union (EU) and providing regulatory oversight to a new industry sector. As technology and innovation have progressed, new entrants to the payment services market have emerged that do not fall within the regulatory framework of PSD.

As a result, the EU has introduced the Second Payment Services Directive (PSD2)¹, which will come into force on **13 January 2018**. The aim is to bring these new market players inside the scope of financial regulation.



In parallel with the EU's initiative under PSD2, the Competition and Markets Authority have mandated the nine main retail banks within the UK to open up the banking market to new entrants. The banks, known as Account Servicing Payment Service Providers (ASPSPs) under PSD2, must allow third-party providers to either facilitate payment transactions or access account information, a process that the Open Banking Group² is helping the banks to deliver.

The principal function of PSD2 is to foster innovation and competition within the European

payments market, while increasing regulatory oversight and ensuring sufficient consumer protection.

Firms who are currently, or wish to start, offering payment initiation or account information services will have to become authorised by the Financial Conduct Authority (FCA) by **13 January 2018**. Following authorisation by the FCA, organisations must then register with the Open Banking Group as well as the individual banks to be granted access, via an Application Programming Interface (API) to the bank's customer payment and account data.

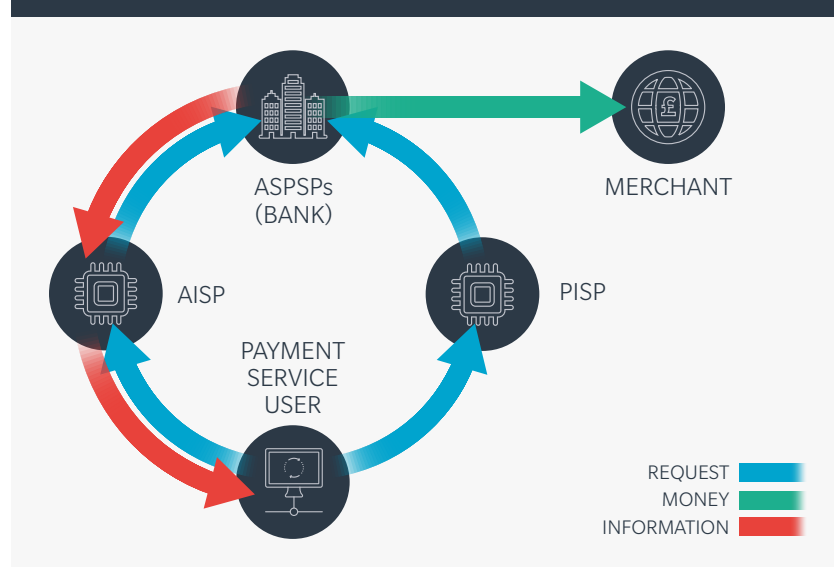
WHO DOES PSD2 AFFECT?

While PSD2 will affect the entire banking and payments industry, arguably the biggest impact will be felt by companies that undertake payment initiation services or account information services via an online platform or mobile application on behalf of individual or corporate users.

PSD2 separates these entities into two distinct categories:

- Payment Initiation Service Providers (PISPs) enable a user to make payment transactions from one or more of their bank accounts held by an ASPSP via a third-party application or platform.
- Account Information Service Providers (AISPs) enable a user to view or aggregate their bank account details and information from an ASPSP into a third-party application or platform for the purpose of managing their budgets or finances.

FIGURE 1 FLOW OF ACCOUNT INFORMATION AND PAYMENT REQUESTS VIA PISPs AND AISPs



Firms that provide both PISP and AISP services will need to apply to the FCA to be authorised in both capacities.

WHAT ARE THE PSD2 REQUIREMENTS?

AUTHENTICATION

New Strong Customer Authentication rules are being introduced and are due to come into force in late 2018, following an initial transition period. This will require multi-step authentication of customer identifiers to reduce the risk of fraudulent account access and ensure the provision of formal customer consent.

DATA PROTECTION

Another requirement of the authentication process for organisations looking to carry out PISP and AISP activities will be to evidence the internal processes in place to monitor and restrict access to sensitive data.

Ensuring adequate data protection and data security standards are in place will be particularly important in light of the EU's upcoming General Data Protection Regulation (GDPR), which is due to come into force on **25 May 2018**. The GDPR greatly increases the liabilities surrounding a data breach and can lead to fines of up to 4% of global turnover.

INSURANCE

One of the most important aspects of PSD2 is ensuring that PISPs and AISPs are able to meet their liabilities to customers and ASPSPs, should there be a claim resulting from the provision of their services.

As a result, as a condition of authorisation by the FCA, PISPs and AISPs are required to put in place adequate professional indemnity insurance (PII), or "a comparable guarantee", to cover potential liabilities.

The European Banking Authority (EBA) has produced some guidance on what the PII should address in order to be suitable for entities covered by PSD2. The EBA has also issued a formula for calculating the minimum monetary limit of the PII based on, amongst other things:

- The number of payment transactions authorised or payment accounts accessed.
- The range of business activities undertaken.
- The volume of clients or value of transactions in a given time period.

Companies can purchase a higher limit of indemnity than the amount calculated by the EBA's formula; however, it is for companies seeking authorisation to demonstrate compliance with the prescribed formula as part of the application process.

AISPs will be required to hold insurance that covers any third-party liability arising from unauthorised access or unauthorised use of a customers' payment account information.

PISPs, by contrast, will be required to hold insurance that covers the cost of reimbursing a third party, where the PISP incurs a liability as a result of:

- Unauthorised payment transactions.
- Late or non-execution of payment transactions.
- Defective execution of payment transactions.

The burden of proof will be on the PISP to demonstrate that the transaction was "authenticated, accurately recorded, and not affected by a technical breakdown or other deficiency".

One of the key insurance criteria that the EBA has indicated in its guidance is that the limit of indemnity (as calculated in accordance with the EBA formula) should not be eroded by non-PSD2 liabilities. Companies may wish to take this into account when considering the suitability of any pre-existing insurance, especially for firms that carry out wider activities beyond those of a PISP or an AISP.

Firms may also wish to consider their wider insurance programme in conjunction with implementing the PII coverage prescribed by PSD2. While a traditional professional indemnity policy will cover the liability towards a third party who has suffered loss as a result of a failure in the provision of services, it will not indemnify a company for loss, costs, or expenses should it fall victim to a cyber-attack or theft.

SUMMARY

The new rules governing payment transactions within the EU come into force on **13 January 2018** and affected organisations should be considering their authorisation requirements.

Marsh has been actively engaging with key stakeholders in developing a solution for the PSD2 insurance requirements and is well positioned to guide clients on the implications of PSD2 for their business and suitable insurance product solutions.

CONTACT

For further information on this subject, please contact:

SHARON KERR

FINPRO UK
+44 (0)20 7357 2861
sharon.kerr@marsh.com

NICOLA BARNETT

FINPRO UK
+44 (0)20 7357 3205
nicola.barnett@marsh.com

1. Incorporated into UK law in the Payment Services Regulations 2017.

2. The Open Banking Group was set up by the main UK banks to assist them with delivering the Competition and Markets Authority's requirements.



The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

In the United Kingdom, Marsh Ltd is authorised and regulated by the Financial Conduct Authority.

Marsh Ltd, trading as Marsh Ireland is authorised by the Financial Conduct Authority in the UK and is regulated by the Central Bank of Ireland for conduct of business rules.

Copyright © 2017 Marsh Ltd. All rights reserved. GRAPHICS NO. 17-1154