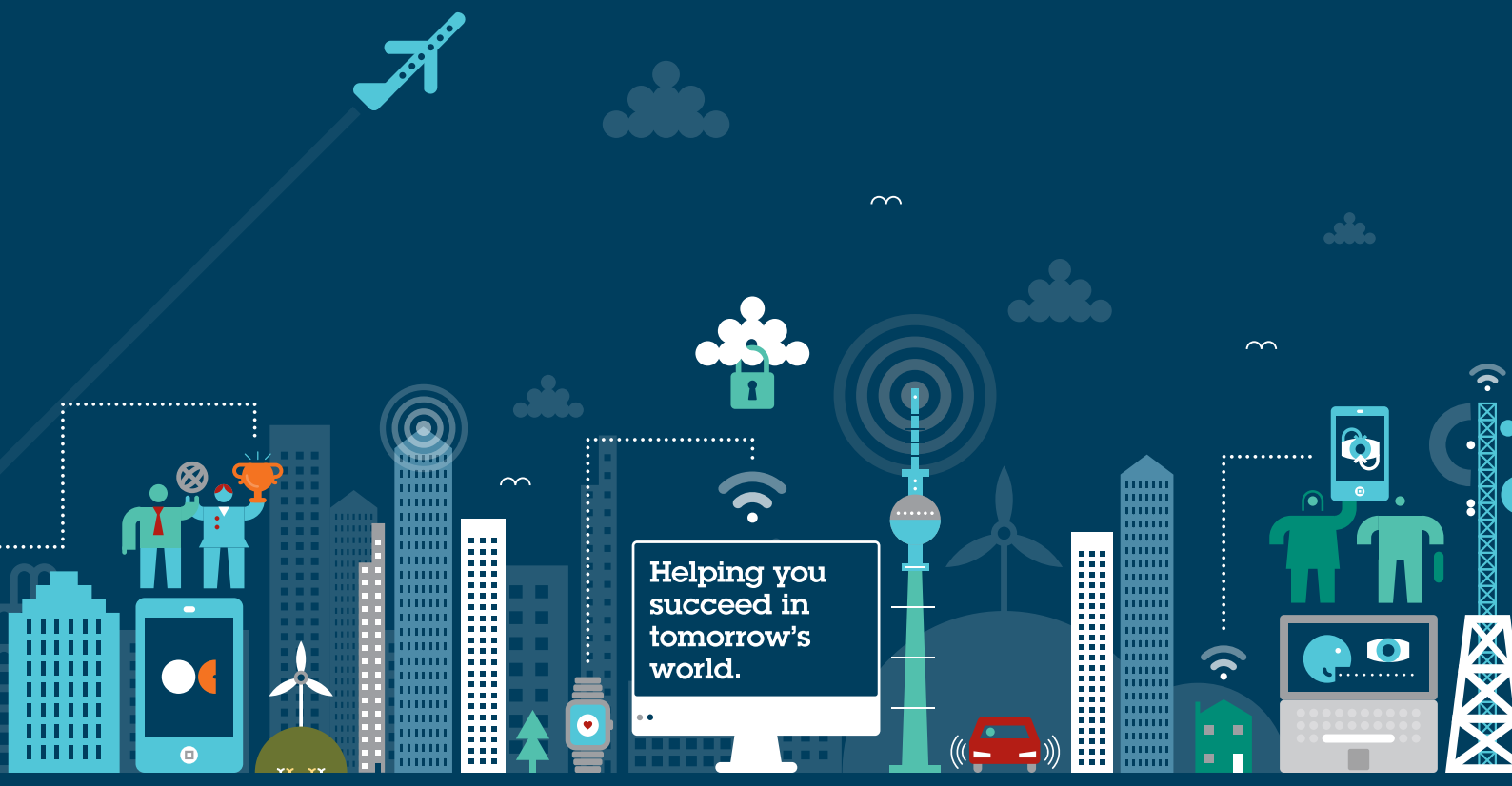
# The Second Payment Services Directive

## The ramifications for existing market players

Osborne Clarke



## Executive summary

The revised EU Payment Services Directive 2015/2366 (**PSD2**) will have significant repercussions for existing payment service providers (**PSPs**) (such as banks, e-money institutions (**EMIs**), payment institutions (**APIs**)) as well as the operators of e-commerce marketplaces and platforms, gift card and loyalty programmes, fuel card operators, bill payment services, digital and mobile wallet services and collections agents, payroll providers and many others. In this guide we focus on considerations for existing PSPs, which include the following:

- **Extension of scope:** the extension in scope both in terms of payment transactions and new payment services will require change not only from an operational perspective but also through revised systems, processes and documentation. Given the importance of the existing exemptions, PSPs will need to assess whether their business still falls within the scope of the exemption or whether changes are required to continue its application.

- **Security:** the changes being introduced to authenticate payments will necessitate a review of existing security and risk management arrangements to ensure they will be fit for purpose but given much of the technical detail in this area is still unclear at the European level, the timetable for implementation is likely to be challenging.

- **Conduct of business:** amendments to conduct of business rules will require PSPs to update existing processes concerning areas such as refunds, surcharges and liability.

- **Passporting:** PSD2 introduces a number of changes intended to harmonise the approach to passporting across the EU and ensure adequate levels of control.

## Legislative background

PSD2, which will replace the original directive, was published in the Official Journal of the EU on 23 December 2015 and must be implemented into national legislation by 13 January 2018.

Like its predecessor, PSD2 will have a significant effect on many in the payments industry – the exact ramifications will depend on the type of PSP and its range of services. A key facet of the revised directive is to address concerns that PSD was not implemented in a harmonised way across all member states.

PSD2 preserves the structure of the original PSD in terms of the split into sections and content areas but has added a number of new or amended provisions. A large number of those changes or amendments are being introduced to address the significant technological developments in retail payment services since the PSD was adopted in 2007. In addition to these technological developments, a number of new types of PSPs have entered the market, which has led to an extension in the scope of regulation, and also measures to level the playing field for different types of PSPs. Other drivers of change include the need to make payments more secure, to introduce additional consumer protection measures, and to encourage lower prices. PSD2 is also an important step towards a Digital Single Market in Europe, which aims to make the EU's single market fit for the digital age.

This guide provides a high level overview of the elements of PSD2 that will affect existing PSPs along with an initial assessment of the potential implications.

## Changes to scope

### Extension of scope: payment transactions

PSD applies to all EEA currency payments where the PSPs of both the payer and payee are located within the EEA. PSD2 will have an expanded scope; also applying, with some exceptions, to:

- non-EEA currency payments between EEA domiciled PSPs; and
- so-called "one-leg out" transactions (where one of the PSPs is located outside of the EEA) in any currency.

This means that many more information and conduct requirements will apply to international payments, and to currency products and services, which were previously excluded from the scope of the regime. PSD2 still enables PSPs to opt out of all information requirements and certain conduct requirements when dealing with business customers (but excluding micro-enterprises) – the corporate 'opt-out'. Nevertheless, these changes should be viewed as putting one-leg out and non-EEA currency payment transactions on an equal footing with EEA transactions as regards:

- the information to be provided before and after the execution of a transaction (Title II) ; and
- the rights and obligations of both the PSP and the customer in relation to those transactions (Title IV) (together, **the conduct of business requirements**).

The extent of the impact of this extension of scope on the information requirements under Title III will depend on the whether the PSP is providing transaction services as part of an on-going relationship under a 'framework contract' or as a single payment transaction, whether there are low value transactions involved and whether the PSP can rely upon the corporate opt-out.

The greater impact is more likely to be felt under Title IV as regards the application of the conduct of business requirements, especially the four execution principles, i.e. the charging principle, the principal preservation principle, execution time requirements and value dating and availability requirements. The application of these principles will vary depending on the PSP's role (for the payer, the payee or as an intermediary), the transaction currency, if any element is out of the EEA and any currency conversion (and if so between which currencies). There are numerous possibilities, each of which requires careful analysis, but one helpful clarification in PSD2 is that FX is out of scope of these principles.

### Extension of scope: new payment services

Given the evolution of the payment services market since 2007, PSD2 introduces two new payment services to cover the activities of so-called 'third party' providers (**TPPs**) who offer payment initiation and account information services.

Until now, TPPs have faced significant barriers to offering their solutions across the EU because of security and secrecy concerns raised by some PSPs. PSD2 seeks to deal with these concerns by bringing TPPs within the scope of regulation and promoting competition by facilitating their operation.

A payment initiation service (**PIS**) is a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP. An account information service (**AIS**) is an online service to provide consolidated information on one or more payment accounts held by the payment service user with another PSP or with more than one PSP.

By bringing TPPs within the scope of regulation, they become subject to authorisation requirements and conduct of business rules, particularly around security and use of data; they also benefit from passporting rights. But to facilitate their operation, PSD2 mandates how account-servicing PSPs must interact with TPPs and it is this aspect that will have the most significant consequences for existing PSPs.

PSPs providing payment accounts that are accessible online (**ASPSPs**) will be required to allow their customers to give providers of PIS and AIS (**PISPs** and **AISPs**) access to their accounts, hence the expression "open access". Such access must only be provided with the user's consent, but cannot be made conditional by the ASPSP having a contract in place with the TPP. This will have a huge effect on systems and processes, as well as documentation (notably customer terms and conditions). For example, ASPSPs will need to put in place operational and IT measures to:

- authenticate the status and identity of each TPP;
- communicate with the TPP in a secure way;
- allow the TPP to rely on its authentication procedures;
- feed account information to, and/or accept payment instructions from, TPPs;
- notify the competent authority (the FCA in the UK) where it denies access to a TPP;
- treat payment orders transmitted through a PISP without any discrimination other than for "objective reasons", in particular in terms of timing, priority or charges, vis-à-vis payment orders received directly from the payer;
- similarly, treat data requests from an AISP without any discrimination other than for "objective reasons"; and
- provide or make available to a PISP all information on the initiation of a payment transaction and all information accessible to the ASPSP regarding its execution.

In addition, PSD2 provides (for the user's protection) that the ASPSP is primarily liable to the customer as regards improper execution and unauthorised transactions when a TPP is involved. Whilst the ASPSP could seek to recover such losses from the TPP, it may not have a direct contractual relationship under which to seek them, though the burden of proof does lie with the TPP to prove authentication of the payment within its 'sphere of competence'. PSD2 leaves open how ASPSPs will in practice recover such losses, and so how much comfort ASPSPs can take from the regulation of TPPs, the robustness of their systems and the insurance cover that TPPs will be required to obtain to cover such losses.

None of this new regime is subject to a general corporate opt-out, all existing ASPSPs will need to to implement these requirements.

## Changes to negative scope

PSD2 contains some amendments to existing exemptions in PSD. The European Commission noted in its review of PSD that certain exemptions had been transposed or applied by Member States in different ways, leading to regulatory arbitrage and legal uncertainty. As a result, PSD2 clarifies and amends some of the existing exemptions as discussed below.

### Limited network exemption

PSD currently provides an exemption for payment services that are based on instruments used to acquire goods or services in or on the issuer's premises or within a limited network of service providers or for limited range of goods or services.

Payment activities covered by the limited network exemption often comprise significant payment volumes and values, as well as hundreds or thousands of different products or services. This was not the original purpose of the limited network exemption. Consequently, this exemption has been significantly narrowed and the circumstances in which a payment instrument should be considered to be used in a limited network are clarified.

The revised exemption now covers services based on specific instruments, designed to address precise needs, which can be used only in a limited way. The instruments either:

- allow the holder to acquire goods or services only in the premises of the issuer, or within a limited network of service providers under a direct commercial agreement with a professional issuer; or

- can be used only to acquire a very limited range of goods or services.

The question of what is meant by 'limited' remains unanswered but the new directive does introduce a new requirement for the relevant regulator to be notified if the total value of transactions in any 12-month period exceeds €1 million. This will create a proactive duty on the regulator to check that the exemption criteria apply to the relevant PSP and it will be required to notify the PSP if it concludes they do not; it is also intended to create transparency and harmony of approach as regards such activities, as the regulators are obliged to publicly disclose descriptions of activities so reported to them. The tightening of this exemption is likely to be real concern for card programmes operating cross-border involving member states whose regulators interpret the application of this exclusion differently. Where a regulator decides that a service doesn't qualify for the exemption, there's no provision for a transitional period (for example, to allow the operator to either obtain full authorisation or become the registered agent of a PSP to continue operating the service, or for an authorised PSP to become the operator (by transfer or otherwise), or for the orderly winding down of the affected scheme).

### Commercial agents exemption

The commercial agents' exemption has been applied very differently across the Member States. According to the recitals to PSD2, e-commerce market places and platforms have unfairly relied on being the agent of both consumer and merchant, rather than of one or the other, to remain outside the scope of PSD. PSD2 narrows this exemption so that it only applies if the commercial agent is authorised to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee.

Where agents act on behalf of both payer and payee, they should be excluded only if they do not at any time enter into possession or control of client funds. The UK government has said that it expects that a number of 'platform' business models which match buyers and sellers for goods and services are unlikely to benefit from the revised exemption and so will now fall within the regulatory scope of the PSD2.

### Electronic communications networks and services exemption

PSD exempted transactions executed by means of, and delivered or used through, telecommunication, digital or IT devices. Under PSD2, only digital content or voice-based services provided via an electronic device as an ancillary service and charged to the related telecoms bill are excluded.

Digital content means goods or service produced and supplied in digital form whose use or consumption is restricted to a technical device. It does not include the use or the consumption of physical goods or services content (such as apps, wallpaper, ringtones, videos, or games). PSD2 does, however, exclude services performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets.

As the intention is for the exemption to be used for lower-value and micro-payments, individual transactions are exempt only if they do not exceed €50 and the cumulative value of payment transactions for an individual subscriber does not exceed €300 per month.

### ATM exemption

PSD exempted cash withdrawal services provided by independent ATM operators but did impose transparency requirements for ATM services offered through banks or other PSPs. PSD2 extends these transparency requirements to include services through independent ATM operators, but does not require independent ATM operators to become authorised. ATM operators falling within the exemption will be required to comply with the basic transparency provisions of PSD2, which will mean the provision of information on withdrawal charges before the withdrawal, as well as on receipt of the cash.

## Other changes to the conduct of business requirements

For the majority of existing PSPs the amendments to the conduct rules (excluding amendments to scope as discussed above) should only require updates to existing processes and documentation, rather than wholesale re-writes. The amendments include changes to:

- **Refunds:** PSD2 improves direct debit refund rights for payers. It brings them in line with debtors' rights under the SEPA core direct debit scheme by granting the payer a "no-questions-asked" refund right within eight weeks of the debit date. PSD2 also gives a refund right in respect of other payments, provided certain conditions are met.

- **Surcharges:** PSD2 is designed to help lower charges for consumers by preventing recipients from adding a 'surcharge' for card payments in the vast majority of cases, both online and in shops. In situations where card charges imposed on merchants are capped (in accordance with the Interchange Fee Regulation), merchants will not be allowed to surcharge consumers for using their payment card.

- **Liability:** The new rules streamline and further harmonise the liability rules in case of unauthorised transactions. Except in cases of fraud or gross negligence by the payer, the maximum amount a payer could, under any circumstances, be obliged to pay in the case of an unauthorised payment transaction will decrease from €150 to €50.

- **Misdirected payments:** If funds have been credited to the wrong account as a result of the customer providing an incorrect unique identifier, a PSP will have to provide the customer with all information relevant to enable it to recover the payment.

### Dispute resolution

Under PSD2, PSPs will be required to put in place adequate and effective internal complaints resolution procedures, and provide related information before a dispute is referred to an Alternative Dispute Resolution (**ADR**) procedure or brought before a court. This includes being required to respond fully in writing to payment complaints within 15 business days of receipt. In exceptional circumstances a holding reply can be provided, explaining the reasons for the delay, with the final response being received within 35 business days. This applies to all users (i.e. there is no corporate opt-out) and so will require changes to customer documentation and processes given that the current requirement is for PSPs to respond to complaints within eight weeks.

Firms are required to ensure the availability of ADR procedures. In the UK, such a system already exists in the form of the Financial Ombudsman Service (**FOS**) and the UK government intends to implement the requirements of PSD2 in this regard through the existing mechanism. PSD2 enables Member States to choose not to implement these ADR procedures for users that are not consumers. To this effect, the UK government has confirmed that it does not intend to extend access to the FOS for businesses that would not usually have such access.

## Security

Security is a key focus of the new directive and PSD2 introduces new requirements relating to operational and security risks. These new security requirements will likely require PSPs to update their procedures, particularly in relation to authentication. The new provisions are summarised below.

### Reporting requirements

All PSPs will need to report major operations or security incidents to the FCA and notify customers directly and without 'undue delay' if a security incident might affect the financial interests of those customers. The European Banking Authority (**EBA**) is required to issue guidelines to help PSPs work out the types of major incidents that would require them to notify a security incident. PSPs will also be required to provide annual information on their assessment of the operational and security risks associated with their payment services and on the adequacy of their risk mitigation and measures and control mechanisms.

For FCA regulated firms, the need to provide details of security arrangements and to report issues to the regulator will be a known condition of doing business. However; the duty to notify customers without 'undue delay' will require further consideration particularly in light of the need to carry out investigations to establish the extent of the breach and identifying appropriate channels for such communications.

### Authentication

A key element of PSD2 is that all PSPs will have to apply "strong customer authentication" (**SCA**) (other than where the EBA permits exceptions) when the payer:

- accesses its payment account online;

- initiates an electronic payment transaction; or

- carries out any action through a remote channel that may imply a risk of payment fraud or other abuses.

SCA means authentication based on the use of two or more elements (which result in an authorisation code) categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data. It must not be possible to forge an authentication code or generate a new code based on knowledge of an earlier code. In particular, where any of the SCA elements or the authentication code is used through a "multi-purpose" device like a mobile phone or tablet, additional security measures should be adopted such as separate secure execution environments installed on the device.

In addition, PSPs must make the payer aware of the amount of the payment and the identity of the payee. In the case of remote electronic payment transactions, SCA must include elements which 'dynamically link' the transaction to a specific amount and a specific payee. Any change in the payment amount must make the authorisation code invalid. PSPs must also ensure the information on the payee and payment amount are kept secure and protected from fraud.

If a payer's PSP does not require SCA, the payer will only be liable for a disputed transaction where it is committing fraud. If the payee or the payee's PSP does not accept SCA, it must refund the financial damage caused to the payer's PSP. PSD2 does not provide for any general exemption from the application of SCA for corporate users (though the relevant liability provisions are subject to corporate opt-out).

### Technical standards

PSD2 requires the EBA to develop (and periodically review) regulatory technical standards (**RTS**) to specify the requirements for SCA and any exemptions from the use of SCA.

The EBA published draft standards for consultation in 2016 with the aim of the final standards being published in January 2017. Their adoption has, however, been delayed due to significant questions being raised by both the European Parliament and over 200 respondents as part of the consultation process. On 23 February 2017, the EBA published a revised, hopefully final draft RTS (**EBA RTS**), which are now with the EU Commission awaiting adoption.

The RTS will apply 18 months after coming into force, so they will not apply until November 2018 at the earliest: much depends on the EU Commission's response which is currently awaited. Unhelpfully this means that firms will be required to comply with the PSD2 provisions on SCA from January 2018, despite the more detailed RTS not being applicable until some months later.

Chapter 3 of the revised draft EBA RTS sets out a number of exemptions that PSPs can rely on. There are various general conditions for the use of these exemptions, essentially to ensure a PSP has in place transaction monitoring mechanisms (see further below). A PSP is not bound to use these exemptions: it may choose to apply SCA on all relevant occasions.

- **Payment account information** – SCA need not be applied where payment service users (PSUs) are limited to accessing an account balance or viewing details of payment transactions executed in the last 90 days (provided the PSU is not accessing the account for the first time or has viewed payment transaction details online in the last 90 days and SCA has been applied within this period).

- **Contactless payments at point of sale** – PSPs are exempt from the application of SCA where the payer initiates a contactless electronic payment transaction provided that: (a) the individual amount of the contactless electronic payment transaction does not exceed €50; and (b) the cumulative amount, or the number, of previous contactless electronic payment transactions initiated via the payment instrument offering a contactless functionality since the last application of SCA does not, respectively, exceed €150 or 5 consecutive individual payment transactions.

- **Transport and parking fares** – SCA need not be applied to electronic transactions at unattended payment terminals for paying for transport or parking fares. The recitals to the EBA RTS explain that this is desirable for operational reasons (to avoid queues and potential accidents at toll gates) or for safety or security reasons (the risk of shoulder surfing). There is no monetary limit for this exemption.

- **Trusted beneficiaries and recurring transactions ('white-lists')** – SCA need not be applied where (i) a payer initiates a payment to one of a list of "trusted beneficiaries" previously created or confirmed by the payer through its ASPSP; and (ii) the payer initiates a series of transactions with the same amount and the same payee. The exemption will not apply to any creation of or use for the first time or amendments to either the list of trusted beneficiaries or the series of payments.

- **Payments to self** – SCA need not be applied to credit transfers initiated by a payer where the payer and the payee are the same person and both payment accounts are held by the same ASPSP.

- **Low-value transactions** – SCA need not be applied to remote electronic payment transactions initiated by a payer which do not exceed €30 individually unless the cumulative amount or number of contactless payments has since the last application of SCA exceeded €150 or 5, respectively.

- **Transaction risk analysis (TRA)** – SCA need not be applied apply to remote electronic transactions which have been identified by the PSP as low risk according to the detailed transaction monitoring mechanisms set out in the EBA RTS. Broadly the amount of the transaction must not exceed the "Exemption Threshold Value/ETV" specified in a table for remote card-based payments and credit transfers (as the case may be) for the corresponding fraud rate (set as a percentage of the relevant category of transactions) and subject to an overall transaction limit of €500. The PSP must have sufficient transaction monitoring mechanisms in place to enable it to perform a real-time risk analysis, taking into account certain specified factors and behaviours and must identify the relevant transaction as 'low risk' only where it meets certain conditions like the absence of any abnormal spending or behavioural pattern or unusual information about the device or access used to initiate the payment transaction. PSPs must monitor their fraud rates as well as the performance of the transaction risk analysis used, which must also be assessed by independent auditors, with their report again available on request to regulators. Lastly, PSPs must notify regulators of their intention to use this TRA exemption and where appropriate also inform users.

It is worth noting that the EBA refused to exempt payments by corporate users, despite numerous comments from respondents during the consultation process. And also that the EBA RTS does not define key expressions like contactless payment, unattended payment terminal, trusted beneficiary, remote electronic payment transactions and remote card-based payments.

In order to rely on any of these exemptions, PSPs must have transaction monitoring mechanisms in place to enable them to detect unauthorised transactions. These mechanisms should include real time risk monitoring which takes into account a number of criteria including a customer's payment transaction history, and spending patterns. PSPs must record and monitor all of their fraud rates as well as the performance of the transaction-risk analysis method used. In addition, security procedures must be documented and periodically tested, as well as being audited by internal or external independent and qualified auditors on at least an annual basis. The report must be made available to regulators on request.

The final draft RTS have been submitted to the EU Commission for adoption, following which they will be subject to scrutiny by the European Parliament and the Council before being published in the Official Journal of the European Union. As noted above, the timing of application is uncertain – the RTS will be applicable 18 months after entry into force, which would suggest an application date of the RTS in November 2018 at the earliest.

## Passporting and cross-border activities

To address identified weaknesses in the current passporting regime, PSD2 introduces a number of changes intended to harmonise the approach across the EU and ensure adequate levels of control. Whilst the relevant provisions refer to payment institutions, EMIs will also be subject to the revisions as a result of PSD2 amending 2EMD to ensure that the articles on passporting under PSD2 apply to EMIs in the same way.

PSD2 sets out a revised process for PSPs to exercise their rights to offer services in other member states on either a branch basis (within 60 days), or cross-border service basis (within 40 days). Banks will continue to passport under a separate, but similar, regime under the Fourth Capital Requirements Directive. However, host states also have the power to require passporting firms to appoint a central point of contact.

Host states can contact the passporting firm's home state regulator with any allegations of non-compliance. This could enable a host state to escalate any differences in its interpretation of PSD2 to the home state regulator, which could undermine the concept of home state control that is especially important for consistency in services provided using agents who refer electronic transactions across borders. In addition, the host state can take precautionary measures in the event of an emergency situation such as a large scale fraud.

The EBA is tasked with producing draft technical standards that will provide greater detail on the framework for co-operation and exchange of information between regulators for passport notifications or supervisory purposes. The EBA is also producing standards determining when the appointment of a central contact point is appropriate.

## UK implementation

On 2 February 2017, HM Treasury published its consultation on PSD2, together with the draft revised Payment Services Regulations (the PSRs 2017). Given that PSD2 is a maximum harmonisation directive, it is not surprising that this consultation does not contain much tailoring for the UK market – any tailoring could only come in the form of modification and/or additions to the FCA Handbook and its Approach Documents which are discussed in more detail below.

It is worth remembering that from the start of this process, the UK government's objective for PSD2 was to align the requirements as far as possible with existing UK practice, with a view to minimising any negative impact on UK industry and consumers while ensuring that the UK could realise the potential benefits related to increased competition and consumer protection. The draft PSRs 2017 published by HM Treasury intend to revoke the existing Payment Services Regulations and replace them with the new set. The government considers that this is likely to make the UK legislation easier to use, principally because large parts of the new draft regulations reproduce the equivalent parts of the old regulations. Many of the current exemptions and derogations exercised under PSD are intended to be retained as a result of implementing PSD2 which limits changes to headline points around the increased scope (in terms of both payment transactions and the new payment services) and the reduced negative scope elements.

Finally, it is worth bearing in mind that the work being undertaken as a result of both the Open Banking Standard and the CMA's retail banking market investigation mean that the government sees PSD2 to as providing the legislative basis upon which its vision for the future of the UK payments market can be built.

On 13 April 2017, the FCA published their consultation paper on their approach to applying the PSRs 2017. This paper proposes a revised Approach Document which will set out the FCA's approach to applying the PSRs 2017 and the amended Electronic Money Regulations 2011. It will be a single document replacing the existing Payment Services and E-Money Approach Documents. As well as the changes necessary as a result of PSD2, the revised Approach Document includes some proposed clarifications of existing guidance and some new guidance, largely in response to the FCA's February 2016 Call for Input on their approach to the current payment services regime. The FCA has also proposed changes to their Handbook. These include changes to the rules, guidance and directions that apply to payment service providers and e-money issuers and to other providers of retail banking services.

In the paper, the Payment Systems Regulator is also consulting on its approach to monitoring and enforcing the four Regulations in the PSRs 2017 that it is the competent authority for.

The consultation will run for eight weeks with the FCA stating that they expect to publish their Policy Statement in Q3 2017. The aim with this timing is to enable the FCA to take into account HM Treasury's thinking post-consultation (though at this stage not its final position) and to put the relevant rules and guidance to the FCA Board in July 2017. As a result, we expect to see legislation laid and final rules issued less than six months ahead of the go live date.

One final point worth mentioning is that the FCA have confirmed that while the legislative framework is still in the process of being finalised, their current consultation is on the basis of the HM Treasury's draft legislation and, where sufficiently developed, draft RTS and Guidelines, in order to give industry as much time as possible to prepare. If changes are made to the draft legislation that affect the proposals set out in the consultation paper, the FCA will reflect these in their final rules, directions and guidance. They will also consult on any further changes where they believe it is appropriate to do so.

## Practical next steps

Although there will continue to be developments around PSD2 over the coming year as we move towards implementation in January 2018, it is important that PSPs start to put together their regulatory change projects (of they have not done so already), so that they will be in a compliant position by the point of implementation.

Whilst implementation will differ depending on the type of PSP and its range of services, what is clear is that implementation will be challenging for all market players, not least because of the curtailed timing between publication of final standards and the go live date. Impact assessments and gap analysis should be finalised shortly so PSPs can begin to consider and implement:

- revisions to (or the introduction of new) processes;
- more robust systems and controls for some PSPs;
- changes to customer terms and conditions; and
- (where relevant) revisions to arrangements and agreements with third parties, such as intermediaries, processors and programme managers.

## Key contacts


**Paul Anning**
**Partner, UK**
T +44 20 7105 7446
paul.anning@osborneclarke.com

**Kate Johnson**
**Partner, UK**
T +44 20 7105 74230
kate.johnson@osborneclarke.com

**Mark Taylor**
**Partner, UK**
T +44 20 7105 7640
mark.taylor@osborneclarke.com

**Joan Carette**
**Partner, Belgium**
T +32 2 515 9326
joan.carette@osborneclarke.com

**Benjamin Docquir**
**Partner, Belgium**
T +32 2 515 9336
benjamin.docquir@osborneclarke.com

**Lise Breteau**
**Partner, France**
T +33 1 84 8 24552
lise.breteau@osborneclarke.com

**Beatrice Delmas-Linel**
**Partner, France**
T +33 1 84 8 24528
beatrice.delmas-linel@osborneclarke.com

**Matthias Terlau**
**Partner, Germany**
T +49 221 5108 4082
matthias.terlau@osborneclarke.com

**Daniel Walter**
**Counsel, Germany**
T +49 221 5108 4316
daniel.walter@osborneclarke.com

**Umberto Piattelli**
**Partner, Italy**
T +39 02 5413 1752
umberto.piattelli@osborneclarke.com

**Stefano Panzini**
**Associate, Italy**
T +39 02 5413 1741
stefano.panzini@osborneclarke.com

**Coen Barneveld Binkhuysen**
**Associate, The Netherlands**
T +31 20 702 8612
cohen.barneveld@osborneclarke.com

**Rafael Garcia Del Poyo**
**Partner, Spain**
T +34 91 576 44 76
rafael.garciadelpoyo@osborneclarke.com

**Samuel Martinez**
**Senior Associate, Spain**
T +34 91 576 44 76
samuel.martinez@osborneclarke.com

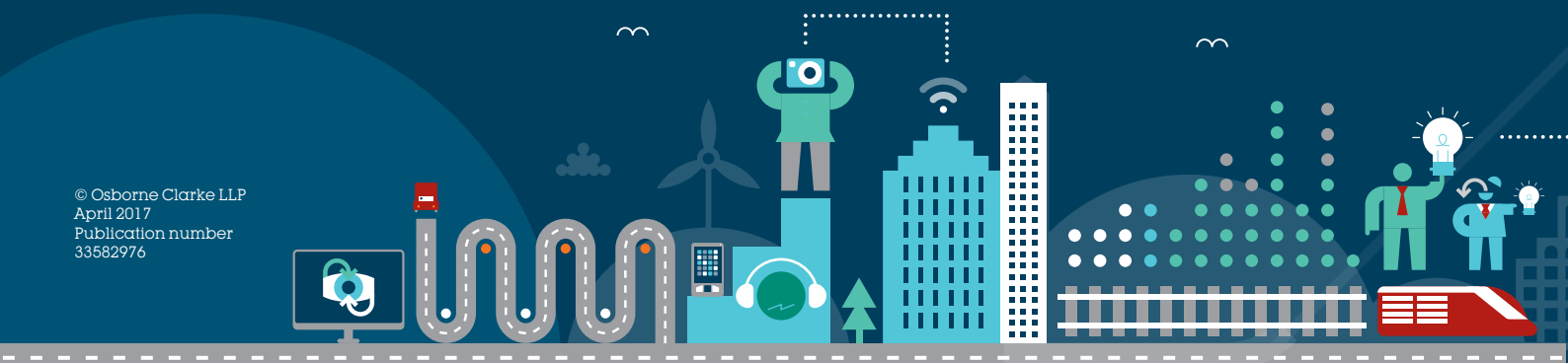

## Where we work

**Belgium:** Brussels
**France:** Paris
**Germany:** Berlin, Cologne, Hamburg, Munich
**Hong Kong**
**India:** Mumbai*
**Italy:** Milan, Brescia, Padua, Rome, Busto Arsizio
**Singapore** ^
**Spain:** Barcelona, Madrid, Zaragoza
**The Netherlands:** Amsterdam
**UK:** London, Bristol, Thames Valley
**USA:** Silicon Valley, New York, San Francisco

Osborne Clarke is the business name for an international legal practice and its associated businesses. Full details here: osborneclarke.com/definitions

*Relationship firm
^An independently owned and managed Singapore law practice

**osborneclarke.com**





April 2017
Publication number
33582976