ParalympicsGB

OFFICIAL PARTNER

Second Payment Services Directive – PSD2

January 2016

Hogan Lovells

13 January 2018: The Clock is Ticking

After a lot of waiting, the date has been set. PSD2 was published in the Official Journal on 23 December 2015 and will come into force on 12 January 2016.

With the exception of some requirements where the implementation period is linked to the finalisation of EBA technical standards, Member States will have until 13 January 2018 to implement the requirements of PSD2.

Key changes

PSD1 started a massive programme of regulatory change for payments that affected nearly all aspects of banking and payment service provision.

The expectation will be that PSD will have a similar impact, as it ushers in:

- Greater information provision and pricing restrictions for international payments.
- A new market for innovators who want to use existing bank and payment infrastructure.
- Significant operational changes for all PSPs.

It will have a major impact on all payment service providers – and on some institutions currently operating outside of PSD1. The impact will be different depending on the type of payment service provider and its range of services. For all, implementation will be challenging.

Key Change	Impact
Scope – One leg out and non-EEA currencies	– More onerous information and conduct requirements – Changes to terms and conditions – Changes to systems and processes – Impact on charging arrangements
Scope – Exemptions	– Less scope to rely on exemptions – New authorisations required – New business models may be needed
Scope – New Payment Services	– New authorisations required – Impact on account providers to allow for effective interaction
Security – Authentication	– New processes required – Changes to terms and conditions – Impact on payees – in particular retailers
Security – Reporting	– New processes required – More robust systems and controls for some PSPs
Passporting	– Potentially more interference from host Member State
Complaints	– Shorter time periods to resolve complaints

Getting ready for implementation

The timetable for implementation is challenging.

With PSD1:

– HM Treasury finalised the regulations 9 months before the implementation deadline.

– The FSA published its draft approach document 7 months before that date.

Implementation programmes had to be well underway before the legislation and approach document were finalised, requiring firms to make massive investments on the basis of assumptions about how the legislation would be implemented.

A similar approach is expected here but with the added complexity of PSD2 leaving much of the detail of certain requirements to EBA technical standards, which will be published around the time of implementation.

A successful implementation project

Against that backdrop, a successful implementation project will require:

– A thorough understanding of the legislation and the wider regulatory environment.

– A detailed understanding of the operational impact on your business – too often the detailed issues are not discovered until late in the day.

– Active engagement with regulators and the EBA through industry bodies.

How we can help

This note provides an overview of the key issues in PSD2.

With one of the largest teams in the City dedicated to payment services, unrivalled PSD1 implementation experience both in the UK and across Europe and close involvement with PSD2 throughout its development, we would be delighted to discuss these issues with you in more detail and help you develop solutions to your PSD2 implementation challenges.

A list of contacts is included at the back of this note.

Increased Scope of PSD 2

Overview

- PSD2 expands the scope of PSD in two ways:
  - By increasing scope to cover international and currency payments.
  - By restricting the scope of some of the existing exemptions.

"One-leg out" and non-EEA currencies

Today PSD only applies if:

- The PSPs of both the payer and the EEA are within the EEA – so-called "one-leg out" transactions where one PSP is outside the EEA are excluded.
- The transaction is in Sterling, Euro or another non-Euro Member State currency. Transactions in all other currencies are out of scope.

Under PSD2, both limitations fall away and the PSD will apply, with some exceptions, to one-leg out transactions *"in respect to those parts of the payment transaction which are carried out in the Union"* and to payments in **any** currency.

This means that many more information and conduct requirements will apply to international payments and currency products and services that were previously excluded from the scope of implementation projects.

Although PSPs will still be able to opt out of all of the information requirements and certain conduct requirements when dealing with business customers (unless they are micro-enterprises), the changes will put these payment transactions on an almost equal footing with EEA transactions.

Impact – One-leg out and non-EEA currencies

Key changes arising from this extension of scope include:

- **Changes to terms and conditions**

  A large number of products and services, particularly USD($) and other currency accounts, were taken out of scope of PSD implementation projects purely because they were foreign currency or one-leg out.

  Those products will now need to be reviewed and their terms and conditions amended to comply with the PSD information requirements.

- **Changes to interest rates**

  PSD1 requires 2 months' notice of changes to contracts unless a change to interest rates is linked to an external reference rate.

  This may require product design changes to link products either to an external rate or, in some cases, to decide not to offer interest at all or to fix rates.

- **Exchange rate transparency**

  Exchange rates will need to be based on a reference rate (although this can be set by the PSP) and there will need to be transparency about it.

  In addition, explicit agreement will be needed to carry out a currency conversion.

- **Charges**

  "SHA" charging will be required for all payments within the EEA (even if there is a currency conversion).

  This means that the payee and payer must pay the charges levied by their own PSP.

  This impacts retail payments and transactions by large corporates.

- **Value Dating**

  Value dating requirements will now apply to all payments wherever they originated.

  This impact is limited to large corporate accounts as other accounts were already subject to a similar rule under BCOBS.

- **Impact on Correspondent Banking**

  Many of these changes are likely to require changes to current correspondent banking arrangements and practices and could impact the commercial pricing of such arrangements.

Exemptions

A number of non-bank institutions, including mobile network operators, currently rely extensively on some of the exclusions from scope in PSD1.

A number of these exemptions will be less useful going forward, notably:

- **The digital download exemption**

  This will be restricted to the purchase of digital content and voice-based services, charitable activities and ticket purchases provided that a single transaction does not exceed € 50 or the cumulative value does not exceed € 300 per month.

- **The limited network exemption**

  This widely used exemption will be restricted to situations where the payment instrument can only be used to acquire a **"very limited range of goods"**.

  In addition, the FCA must be notified if the total value of transactions in any 12 month period exceeds €1 million.

  This creates a proactive duty on the regulator to check that the provider is right to rely on the exemption.

- **The commercial agent exemption**

  The commercial agent exemption has been relied on by a number of payment intermediaries particularly in the download market.

  It will now be restricted to payment transactions through a commercial agent authorised to **negotiate or conclude the sale or purchase of goods or services** on behalf of only the payer or only the payee.

  Just acting as an intermediary with no real ability to negotiate will not be sufficient.

Impact – Exemptions

Businesses that currently rely on these exemptions will need to decide whether they can continue to operate outside of the PSD regime.

Some will need to apply for authorisation as payment institutions whilst others will need to change the basis on which they operate and potentially partner with an authorised PSP.

Either way, many more products and services are likely to come within the scope of PSD as a result of these restrictions on the current use of exemptions.

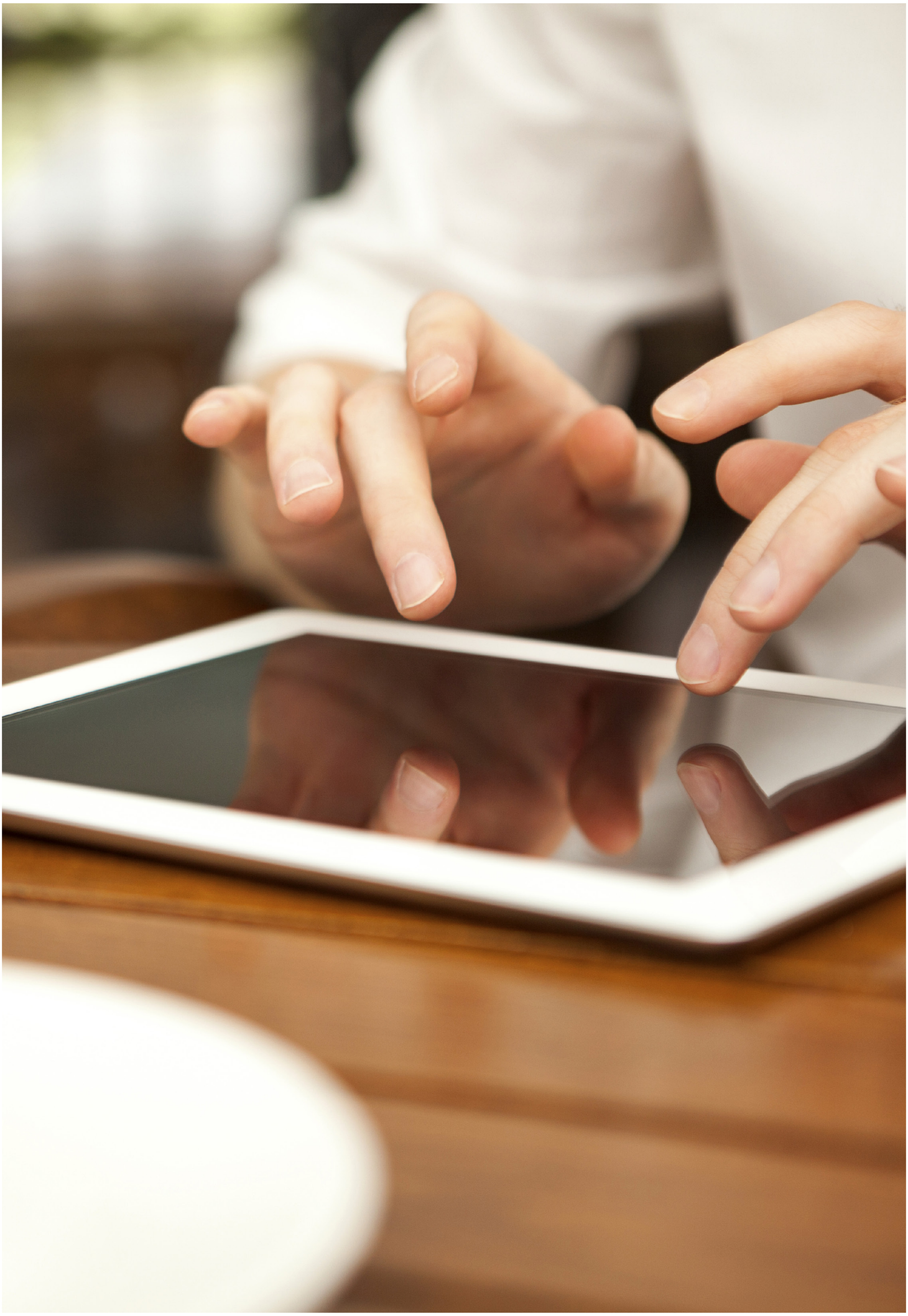
What should you do now? – One-leg out and non-EEA currencies

- Identify accounts and services that will be impacted for the first time
- What changes will be needed to terms?
- Are they cosmetic or is there a commercial impact?
- Establish impact on operations
- Can you provide the additional information?
- Do you need to change your interest or exchange rate basis?
- Can you apply conduct provisions?
- Are new systems and proceeses required?
- Identify reliance on correspondent banks
- Does the existing process allow you to comply?
- If not, what changes need to be made?
- Do they impact the commercial arrangements?
- If you act as a correspondent bank, consider impact for your clients
- Is your service compliant?
- If not, what changes will you need to make?

What should you do now? – Exemptions

If you rely on any of these exemptions you need to:

- Assess whether your business still falls within the scope of the exemption
- For example, what range of goods can be purchased? Is it really “very limited”?
- If the answer is clearly no then you will need to become authorised
- There are no transitional arrangements so work on becoming authorised will need to start straightaway
- If authorisation is not an option you will need to think about how your service can be changed
- Is it possible to change the service to fall within the exemption?
- Is partnering with an authorised institution an option?



The Introduction of TPPs: Third Party PSPs

The Introduction of TPPs: Third Party PSPs

New payment services

PSD2 attempts to deal with the pace of payments innovation by introducing two new payment services to cover the activity of so-called TPPs:

- **Payment initiation services**

  "a service to **initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider"**.

  This will cover services such as SOFORT in Germany and iDEAL in the Netherlands, enabling a customer to log in directly to their bank account via a third party in order to make an online purchase.

- **Account information services**

  "an **online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider"**.

  This will cover account aggregation services which provide consumers with a consolidated view of their bank accounts and enable them to access them by online login.

Impact of PSD2

PSD2 attempts to do 2 things in relation to TPPs:

- **Bring them within the scope of regulation**

  These services are already provided in a number of Member States, often on an unregulated basis.

  The first objective of PSD2 is to ensure they are brought within the scope of regulation.

  Anyone providing one of these services will need to become authorised as a payment institution.

- **Promote competition by facilitating their operation**

  A second objective is to make it easier for these TPPs to operate by mandating how account PSPs must interact with them.

  This area will be of particular concern for existing PSPs and is likely to be a major focus of implementation projects.

Impact for account PSPs – Access

PSPs providing payment accounts which are accessible online, will be required to allow their customers to give TPPs access to their accounts.

This will mean, for example, that banks will no longer be permitted to prohibit the use of account aggregation services.

But it will also have significant operational and systems impacts:

- Payment initiation services who provide card-based instruments must be given information about the availability of funds for a transaction.
- Data requests from an account information service provider must be acted on without discrimination other than for "objective reasons".
- The PSP providing the payment account will need to put in place operational and IT measures to:
  - authenticate the status and identity of TPPs
  - allow the TPP to rely on its authentication procedures
  - feed account information to TPPs, and
  - accept instructions from TPPs.

Impact for account PSPs – Liability

Ensuring the right PSP bears the cost of improper execution and unauthorised transactions involving TPPs will be challenging:

- The PSP providing the payment account is primarily liable to the customer.
- The burden is on the TPP to prove authentication etc of the payment but only within its "sphere of competence".
- The PSP providing the payment account can seek to recover from the TPP but will have no direct contractual relationship.
- To protect against credit risk, TPPs will be required to have insurance but will this be available and how closely will it be monitored? Will it be sufficient?

What should you do now?

Although there are a number of account information service providers operating in the UK whether or not payment initiation service providers will disrupt the UK payments market remains to be seen.

Irrespective of this, there are potentially huge operational changes required for banks and others to ensure they can allow access to TPPs.

- The industry needs to engage with the EBA to achieve workable solutions to common secure standards of communication.
- IT systems will need to be looked at in light of the need to authenticate, identify and exchange information with a range of new PSPs.
- Wide ranging analysis will need to be undertaken to ensure PSPs can meet the demands of TPPs. Owing to the long lead times that IT and operational changes often require, this work should begin in earnest if it hasn't already.

Security

Overview

Security is another key focus of PSD2 and will introduce major changes to the way that PSPs authenticate payments. There is, however, ambiguity around some of the requirements and what these will mean in practice for PSPs.

Strong customer authentication

Other than where the EBA permits exceptions, all PSPs (including TPPs) must use "strong customer authentication" when a payer:

- Accesses a payment account online
- Initiates an electronic payment transaction, or
- Carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

In addition where a payment is electronically initiated elements of the strong authentication must be "dynamically linked" to a specific amount and a specific payee.

Strong customer authentication means authentication based on the use of two or more elements categorised as knowledge, possession and inherence that are independent. That means the breach of one should not compromise the reliability of the others.

If a PSP does not require strong customer authentication the payer will only be liable for a disputed transaction where they are committing fraud. If the payee's PSP does not accept strong customer authentication then they will be liable for any unauthorised transaction – similar to the current liability model for 3-D secure transactions.

EBA Technical Standards

The EBA will work with the ECB to develop, and periodically review, technical standards specifying:

- Requirements for strong customer authentication.
- Any exemptions from the use of strong customer authentication.
- Requirements to protect confidentiality and the integrity of security credentials.
- Requirements for common and secure open standards to enable all types of PSPs to implement the measures effectively.

Although PSD2 reflects the strong customer authentication requirements already in place through the SecuRe Pay recommendations, the drafting style of technical standards is more robust and should provide greater certainty as to what is required – although some will see this as reduced flexibility.

Technical standards are directly applicable in Member States and breach of a technical standard will be a matter for the local regulator.

Because of the need for technical standards these provisions will not come into force until 18 months after the technical standards are finalised.

Impact – Strong customer authentication

- All PSPs, including TPPs, will need to ensure that they comply with the new "strong customer authentication" requirements for all the potential types of payments within scope:
  - It is not sufficient just to focus on internet payments.
  - EBA exemptions will be required for transactions such as contactless payments.
- Some PSPs may already have compliant systems – for example, those who currently use PINsentry type mechanisms to access online banking.
  - Within the UK, solutions are being considered in a number of sectors.
  - But PSP account providers will need to put in place systems which allow a TPP to rely on their authentication method.
- Retailers may be concerned that a customer's check-out experience may be more cumbersome leading to aborted sales.
  - Any solutions will need to be easy to use to deal with these concerns.
- Merchant agreements and card scheme rules will need to be amended to reflect the mandatory nature of the provisions although many retailers will hope that the EBA's technical standards will provide flexibility where they have robust fraud controls in place.

Security – Reporting requirements

There are additions to the information that applicants to be a new PI will have to provide – in particular, they will need to put together:

- A security policy document and a detailed risk assessment in relation to their payment services.
- A description of security control and mitigation measures taken to adequately protect customers against risks such as fraud and illegal use of data.

All PSPs will need to report security incidents to the authorities in accordance with the network and information security ("NIS") Directive.

If a security incident might impact the financial interests of customers, the PSP must also:

- Directly notify **customers** affected "without undue delay", and
- Inform them of measures they can adopt to mitigate the adverse effects.

The EBA will issue guidelines to help PSPs determine when they need to report security incidents.

There are new annual reporting requirements for all PSPs. This includes the need for an updated assessment of the operational and security risks associated with the payment services provided and the adequacy of the mitigation measures and controls implemented in response to such risks.

Impact – Security – Reporting requirements

- FCA regulated firms are already required to provide details of their security arrangements – the new requirements provide a structure for all PSPs.
- Reporting issues to the FCA and, for banks, the PRA will be standard practice. Again this requirement extends to all PSPs.
- Of more concern may be the requirement to inform customers "without undue delay" with, perhaps, companies more likely to revert to the media in a similar way to the TalkTalk incident following their recent data security issues.

What should you do now?

- Identify where strong customer authentication is not currently used:
  - Identify how it can be implemented.
  - If not, will the service need to be withdrawn?
- Identify areas for engagement with the EBA on the development of the technical standards.
- Identify how to report incidents quickly to customers.
- Review existing security and risk management arrangements and ensure that you can evidence effectively that they are fit for purpose.

Other Points to Note

Overview

There are a number of other changes that will be brought in by PSD2. Not all of them are set out in this note but we have highlighted some further important changes in this section.

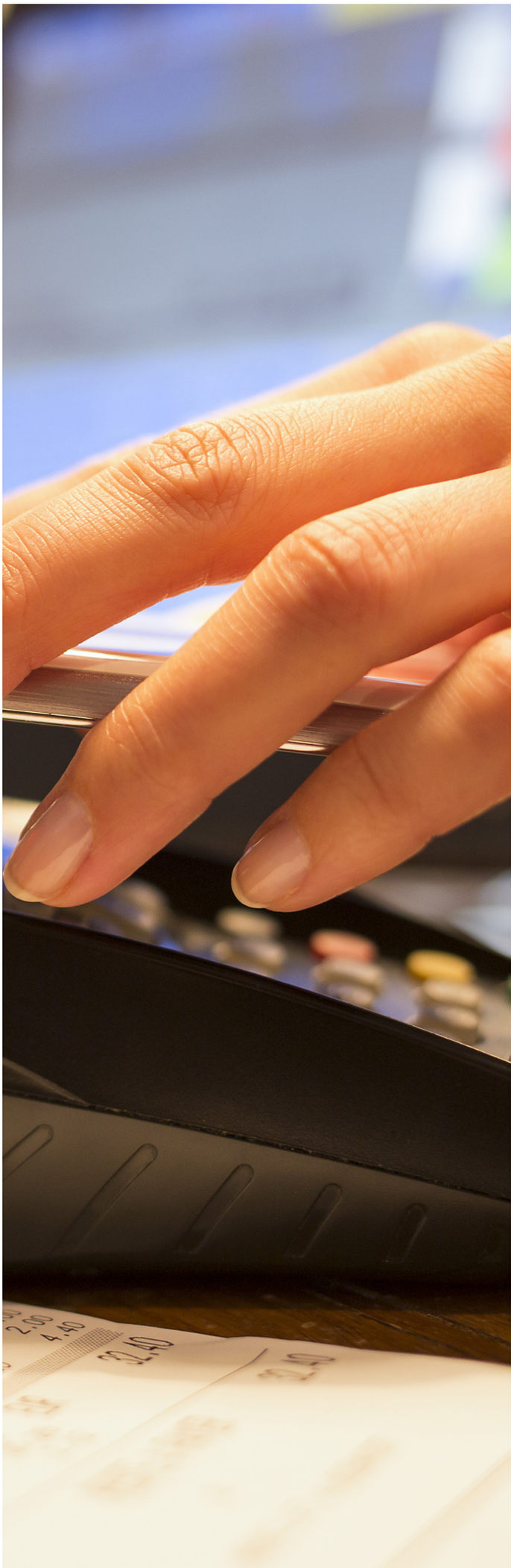
Passporting for payment institutions

To address concerns over the effectiveness of the current passporting regime or payment institutions, PSD2 details a number of changes intended to harmonise the approach across the EU and ensure adequate levels of control.

- Payment institutions wishing to provide payment services under the right of establishment must provide the home Member State with information about their operations.
- The home Member State must then send this information to the competent authorities of the host Member State within one month.
  - This is the same requirement that currently applies to those operating on a cross border services basis.
- Following this, the host Member State has one month to assess the information and provide the home Member State with relevant information in connection with the intended provision of the payment services.
- If the home Member State disagrees with the assessment, it must provide the host Member State with reasons for their decision. Overall, the home Member State has three months from the receipt of information from the payment institution to communicate their decision to both the host Member State and the payment institution.
- The host Member State can require payment institutions that have agents or branches within that Member State to report to them periodically. The reports are only for information or statistical purposes but can, if the right of establishment is used, also be used to monitor compliance with the relevant provisions of national law.
- In addition, Member States can require payment institutions operating in their territory through agents under the right of establishment (with their head office in a different Member State) to appoint a central contact point in their territory. This is to ensure adequate communication and information reporting on compliance and to help supervision by the competent authorities.
- If the host Member State decides a payment institution with agents or branches in its territory is non-compliant, it must inform the home Member State without delay.
- In an emergency situation where immediate action is necessary to address a serious threat to the collective interest of payment service users in the host Member State, the host Member State may take precautionary measures.
  - These measures must be appropriate, proportionate and temporary (and must be terminated when the serious threats are addressed).
  - The measures must not result in preferential treatment of the payment service users of the payment institution in the host Member State compared to those users in the home Member State.
  - Measures should be properly justified and communicated to the payment institution concerned.

Complaints procedure

- PSPs must put in place “adequate and effective” internal complaints resolution procedures, and provide related information.
- This includes having to respond fully to complaints in writing within 15 business days. In “exceptional circumstances”, where the answer cannot be given within this timescale for reasons beyond the control of the PSP, a holding reply will need to be sent to customers clearly indicating the reasons for the delay and specifying a deadline by which the PSP will respond fully to the complaint.



– The deadline for the final written response can't be more than **35 business days** after receipt of the complaint.
– This is likely to require changes to customer documentation and procedure. The current requirement is for PSPs to respond to complaints within eight weeks.

Merchant acquiring

PSD has always regulated merchant acquiring but, because PSD erroneously treated card transactions as similar to direct debits, there has been considerable uncertainty as to how the requirements applied.

PSD2 introduces a new broad definition of merchant acquiring which should assist in identifying whether or not those who provide point of sale payments solutions outside the traditional card acquiring models are caught by the requirements.

Unfortunately, PSD2 has not taken the opportunity to clarify exactly how card acquiring operates and how the requirements are intended to apply so we expect uncertainty to continue in this respect.

Our Team

Emily Reid
Partner, London
T +44 20 7296 5362
emily.reid@hoganlovells.com

Roger Tym
Partner, London
T +44 20 7296 2470
roger.tym@hoganlovells.com

Jonathan Chertkow
Partner, London
T +44 20 7296 2191
jonathan.chertkow@hoganlovells.com

Julie Patient
Counsel, London
T +44 20 7296 5790
julie.patient@hoganlovells.com

James Black
Senior Associate, London
T +44 20 7296 5898
james.black@hoganlovells.com

Charles Elliott
Senior Associate, London
T +44 20 7296 5237
charles.elliott@hoganlovells.com

Peter Finch
Associate, London
T +44 20 7296 5052
peter.finch@hoganlovells.com

Eimear O'Brien
Associate, London
T +44 20 7296 5350
eimear.obrien@hoganlovells.com

Rachel Savary
Associate, London
T +44 20 7296 5342
rachel.savary@hoganlovells.com

Claire Loughrey
Associate, London
T +44 20 7296 5142
claire.loughrey@hoganlovells.com

Stephen Timbrell
Associate, London
T +44 20 7296 5571
stephen.timbrell@hoganlovells.com

Catherine Hayward-Hughes
Associate, London
T +44 20 7296 5520
catherine.hayward-hughes@hoganlovells.com

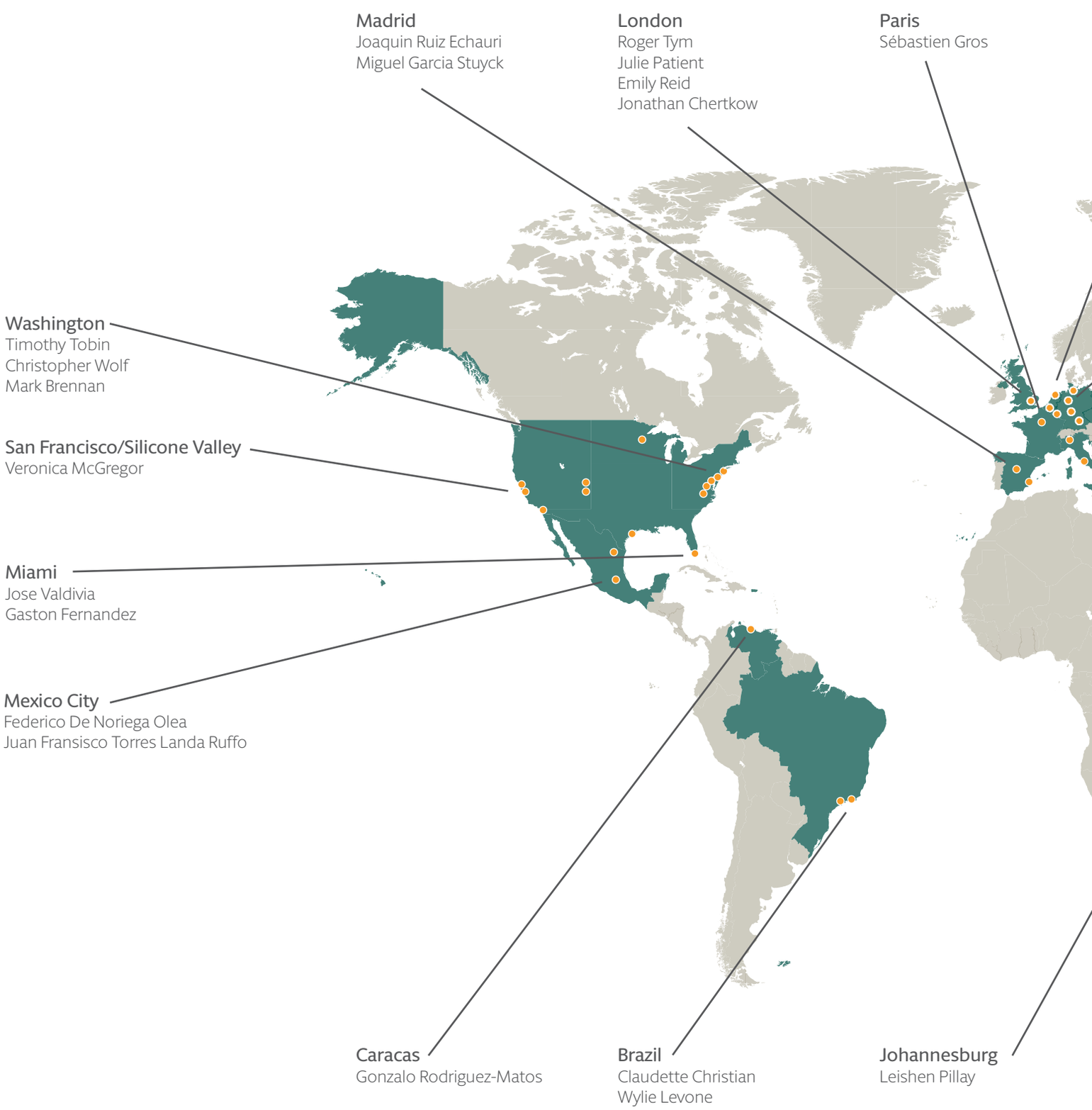
Stephanie Jackson
Associate, London
T +44 20 7296 5688
stephanie.jackson@hoganlovells.com

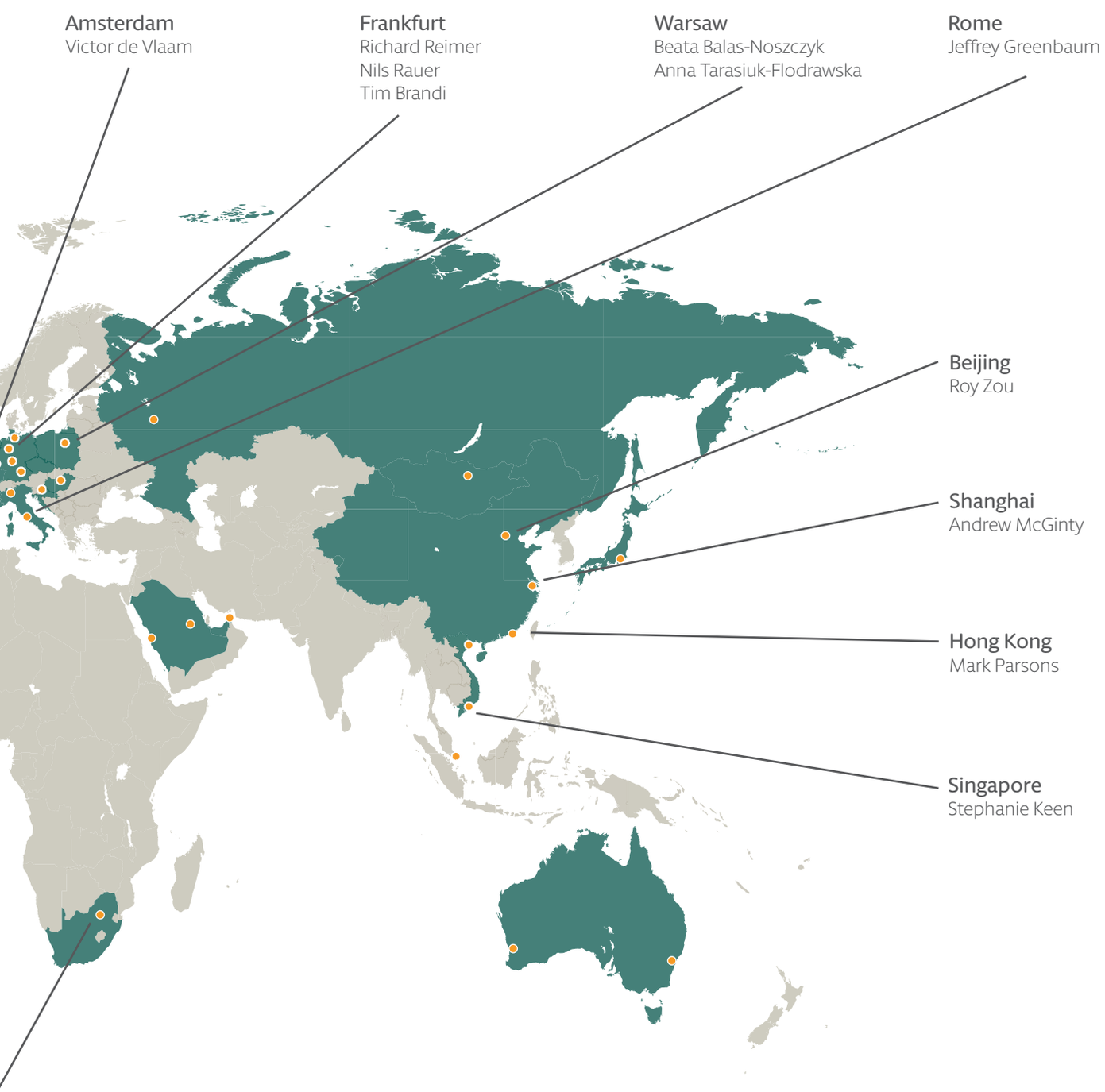
Neelam Hundal
Associate, London
T +44 20 7296 5685
neelam.hundal@hoganlovells.com

Elizabeth Greaves
Associate, London
T +44 20 7296 5635
elizabeth.greaves@hoganlovells.com

Michael Oxlade
Associate, London
T +44 20 7296 5909
michael.oxlade@hoganlovells.com

Local Contacts





Notes

Alicante
Amsterdam
Baltimore
Beijing
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jeddah
Johannesburg
London
Los Angeles
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Riyadh
Rome
San Francisco
São Paulo
Shanghai
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com