Briefing on EU proposals for a second Payment Services Directive and new Interchange Regulation

15 August 2013

Contents
Introduction 1
Overview 1
PSD2
Changes to Scope 1
Changes to conduct of business requirements 3
Agents, passporting and safeguarding 6
Interchange Regulation
Scope 6
Caps on Interchange Fees 7
Removal of Card Scheme Restrictions 7
Transparency 7
INTRODUCTION
On 24 July 2013, the European Union ("EU") published proposals for:

• a second Payment Services Directive ("PSD2") (see here)
• a Regulation on interchange fees for card based payment transactions (the "Interchange Regulation") (see here)

Both proposals will lead to substantial changes to processes and terms and conditions for payment service providers ("PSPs") and will bring some businesses and products within the scope of regulation for the first time.

The subject matter of the proposals is technically complex and not always fully understood by those drafting the legislation. To avoid the problems that have plagued the existing Payment Services Directive ("PSD1"), it is essential that the industry engage closely (and early) in the legislative process.

The proposed timing - adoption by Spring 2014 - is ambitious, particularly with European Parliament elections next summer, and gives the industry little time to have its voice heard. In reality, 2015 may be more realistic. Member States will then have 2 years to implement PSD2. The Interchange Regulation will take effect immediately, although the key proposals for capping interchange will not come into effect for 2 months (for cross-border transactions) and 2 years (for domestic transactions).

OVERVIEW
The PSD2 proposals will amend and replace PSD1 (see here) (article 101). They are aimed at levelling the playing field for different types of PSP, filling gaps in consumer protection, improving the security of payments, reducing areas of ambiguity, and ensuring greater consistency of approach to regulation across the EU.

The Interchange Regulation is designed to complement PSD2 by removing obstacles to achieving a single card payments market, improving transparency of pricing, and addressing competition concerns that the European Commission has been investigating for many years. It is drafted to be consistent with the PSD.

A summary table of key changes accompanies this note.

Key changes
• Changes to scope
• Changes to the conduct of business regime, including on security, liability, access to third party payment service providers, and complaints handling
• Changes to agent, passporting and safeguarding requirements
• Caps on domestic and cross-border interchange fees
• Removal of certain card scheme restrictions
• Increased transparency about levels of interchange fees

PSD2

CHANGES TO SCOPE
PSD2 makes a number of important changes to the scope of PSD1, including:

• extending information requirements to payments in non-European Economic Area ("EEA") currencies and to payments between EEA and non-EEA countries;
• amending the "limited network" and "digital download" exemptions (it also appears intended to narrow the "commercial agents" exemption), and removing the exemption for independent ATM providers; and
• addition of new types of regulated "overlay" payment service, whereby a "third party payment service provider" ("TPP") does not execute funds transfers, but rather provides "payment initiation" or "account information" services in relation to payment accounts provided by other PSPs (the "account servicing PSPs").

One leg out and non-EEA currency transactions
Where funds are sent to or received from a PSP established outside of the EEA (so called "one leg out" transactions), or where payments are executed in non-EEA currencies, they largely fall outside of PSD1.
In future, the information requirements in Title III will apply to them, including requirements on provision of contract terms and other information to customers, variation of such contract terms or information, and termination of customer contracts (article 2).

PSPs will accordingly need to update their customer terms and conditions and processes for such payment services so that they comply with information, variation and termination requirements under PSD2.

However, PSPs will still be able to opt out of the Title III requirements when dealing with business customers (unless they are micro-enterprises).

**New payment services**

PSD2 introduces two new forms of payments service provided by TPPs:

- Payment initiation services
- Account information services

A payment initiation service is defined as "a payment service enabling access to a payment account provided by a third party payment service provider, where the payer can be actively involved in the payment initiation or the third party payment service provider's software, or where payment instruments can be used by the payer or the payee to transmit the payer's credentials to the account servicing payment service provider" (article 4(32) and paragraph 7 of Annex 1).

We expect the intent is to cover services such as iDEAL in the Netherlands, enabling a customer to log in directly to their bank account in order to make an online purchase. However, the vagueness of the drafting is such that a wider set of activities may be caught, arguably including even the storage by online merchants of card details for future payments.

An account information service is defined as "a payment service enabling access to one or more payment accounts by a third party payment service provider to provide internet-based aggregation services where information is collected from one or more payment accounts under disposition by a payment service user with one or more account servicing payment service providers" (article 4(33) and paragraph 7 of Annex 1). It seems clear that this is intended to cover account aggregation services.

**Limited network exemption**

Significant changes have been proposed to the scope of this exemption, which will mean that many currently unregulated products will, in the future, fall within scope of PSD2.

The exemption now covers "services based on specific instruments that are designed to address precise needs that can be used only in a limited way, because they allow the specific instrument holder to acquire goods or services only in the premises of the issuer or within a limited network of service providers under direct commercial agreement with a professional issuer or because they can be used only to acquire a limited range of goods or services" (article 3(k)).

On the face of it, the requirement to "address precise needs", in particular, would significantly narrow the existing exemption, and might be particularly problematic for products such as prepaid store cards or multi-purpose gift cards. However, it is unclear from the drafting whether or not that requirement is intended to add to, or simply to explain, the latter part of the exemption, which refers to "[used] only in the premises of the issuer or within a limited network of service providers ... [or] used only to acquire a limited range of goods or services", and so which reflects the existing language of the exemption in PSD1.

Where the monthly volume of transactions exceeds €1m, a provider will need to seek clearance from the relevant authorities as to whether or not the exemption applies (articles 27(1) and 30(2)). The trigger for seeking clearance is unclear in certain respects, for example, does it relate to the volume of transactions for a particular service, or the volume of all transactions for all services provided by an entity? Who are the "competent authorities" if the provider operates in a number of countries — is it just a regulator in its home State or (more likely) does it need clearance from the relevant authorities in each of the countries? In any case, the introduction of a clearance requirement means that, in future, national authorities are much more likely to turn their minds to considering whether and when the exemption applies, and to challenge providers (and as appropriate to refuse them clearance) when it considers that it does not.

**Download exemption**

This exemption has also been narrowed. It now covers "payment transactions carried out by a provider of electronic communication networks or services where the transaction is provided for a subscriber to the network or service and for purchase of digital content as ancillary services to electronic communications services, regardless of the device used for the purchase or consumption of the content, provided that the value of any single payment transaction does not exceed EUR 50 and the cumulative value of payment transactions does not exceed EUR 200 in any billing month" (article 3(l)).

Unlike the existing exemption, which is available to digital and IT operators as well as telecoms operators,
the new exemption is much narrower so that it is available to telecoms operators alone, and then only for purchase of ancillary digital content of limited value. This will mean that the exemption can no longer cover, for example, accounts offered by online retailers to pay for a wide range of downloads.

**Independent ATM provider exemption**

The existing exemption has been abolished. Currently the exemption is set out in article 3(o) of PSD1, and covers "services by providers to withdraw cash by means of automated teller machines acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account, on condition that these providers do not conduct other payment services as listed in the Annex."

The logic for deletion, in recital (14), is that the exemption was "originally devised as [an] incentive to install stand-alone ATMs in remote and poorly populated areas by allowing them to charge extra fees ... the provision was not intended to be used by ATM providers with networks comprising hundreds or even thousands of ATMs, covering one or more Member States. It leads to non-application of that Directive to a growing part of the ATM market, with negative effects on the consumer protection. It also incentivises the existing ATM providers to redesign their business model ... in order to charge higher fees directly on the consumers."

**Commercial agent exemption**

It seems there is also an intention to narrow the scope of the "commercial agent" exemption in article 3(b). According to recital (11), "The exemption ... is being applied very differently in the Member States. Certain Member States allow the use of the exemption by e-commerce platforms that act as an intermediary on behalf of both individual buyers and sellers without a real margin to negotiate or conclude the sale or purchase of goods or services. That goes beyond the intended scope of the exemption and may increase risks for consumers... Different application practices also distort competition in the payment market. The definition should become more precise and clearer to address these concerns."

In spite of this, the language of article 3(b) has not materially changed, and refers to "payment transactions from the payer to the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of either the payer or the payee". Indeed, the only change is the addition of the word "either". It remains to be seen whether there has been a drafting oversight in not amending article 3(b), or whether instead recital (11) needs changing.

**Potential responses to changes in scope**

The introduction of new, regulated payment services (namely, "payment initiation" and "account information" services), and changes to existing exemptions, means that providers which are currently not authorised as a payment institution ("PI"), or as another form of regulated entity, may need to apply for authorisation. Alternatively, they may choose to change their existing business models, or even to discontinue existing services, in order to avoid the need for authorisation.

The second E-Money Directive ("2EMD") (see [here](#)) incorporates the "limited network" and "download" exemptions by cross-reference to PSD1, and so it seems that changes to those exemptions under PSD2 will be carried across to the e-money regime. This will mean that prepaid products which are currently exempt may become regulated e-money following implementation of PSD2, in which case the provider may need to become authorised as an electronic money institution ("EMI"), if it is not one already, unless it changes the product or discontinues it.

PSPs that are already regulated may today provide a mix of regulated and unregulated services, in which case they also need to consider whether to treat their unregulated services as regulated payment services (or e-money) going forwards, or whether they prefer to change their existing business models in order to maintain services as unregulated, or to discontinue existing services.

**Changes to conduct of business requirements**

PSD2 makes a number of changes to the conduct of business requirements of PSD1, including:

- introducing significant new security requirements, which will require operational changes to be implemented by many PSPs
- making a number of changes to the provisions dealing with liability for unauthorised and improperly executed payments, including to reflect the introduction of new security requirements and the involvement of TPPs
- new measures to provide access to TPPs and facilitate the provision of their services
- new requirements in relation to complaints
Security: strong customer authentication

Account servicing PSPs will need to implement "strong customer authentication" when a payer initiates an electronic payment transaction, except where an exemption is permitted under guidelines to be published by the European Banking Authority ("EBA") (article 87). The scope of this requirement needs clarifying - it is unclear what is meant by "electronic" transactions (it could arguably include many forms of face-to-face transaction), and it remains to be seen which exemptions the EBA will permit.

Strong customer authentication means "a procedure for the validation of the identification of a natural or legal person based on the use of two or more elements categorised as knowledge, possession and inherence whereas the selected elements must be mutually independent, in that the breach of one does not compromise the reliability of the other(s)" (article 4(22)).

This may require many PSPs to upgrade their current procedures so that customers can authenticate their transactions on the basis of, for example, password + security token, or PIN + card or phone, or password + fingerprint. It reflects the strong customer authentication requirements already in the SecuRe Pay recommendations published by the European Central Bank ("ECB") (see here), which PSPs will need to implement by February 2015.

The EBA will work with the ECB to develop, and periodically review, guidelines:

• for establishing and monitoring security measures, "including certification processes where relevant" (article 86(2),(3)); and

• on state of the art customer authentication, and any exemptions from the use of strong customer authentication (article 87(3)).

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, and a description of security control and mitigation measures taken to adequately protect customers against risks such as fraud and illegal use of data (article 5). These changes will be incorporated by cross reference into 2EMD, and so will also apply to entities applying to be an EMI.

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 the customers affected "without undue delay", and inform them of measures they can adopt to mitigate the adverse effects (article 85). The EBA will issue guidelines to help PSPs determine when they need to report security incidents (article 86(4)).

There are new annual reporting requirements for all PIs in relation to security. 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 (article 86(1)).

Liability: improper execution and unauthorised transactions

Where a payment transaction is executed late, rather than being sent to the wrong payee, the payer may decide that the amount is to be value dated on the payee's account by the date it should have been received, instead of receiving a refund. How this will work in practice will need consideration, as it puts the onus on the payee's PSP to adjust the payee's account even though the payer's PSP or a TPP may be liable for late execution (article 80). Operational changes are likely to be required at a payment scheme level to facilitate this right.

There are also some changes to the liability regime for unauthorised payments:

• The maximum liability that can be imposed on a payer when not at fault for a lost, stolen or misappropriated payment instrument has been reduced from €150 to €50 (article 66(1)).

• The terms governing a customer's use of a payment instrument must be "objective, non-discriminatory and proportionate" (article 61(1)). This is presumably aimed at ensuring that PSPs do not impose unduly onerous security requirements on customers. It is important because a customer can be made liable for all unauthorised transactions arising as a result of intentionally or grossly negligently failing to comply with terms governing use of their payment instrument, up until the time of notifying the PSP of its unauthorised use (article 66(1),(2)).

• Where "strong customer authentication" has been used for a transaction made via a distance communication (e.g. any online purchase), then it appears that the payer can now be made liable if the transaction is unauthorised as a result of the payer having been grossly negligent in meeting their security obligations – this is not currently the case under
distance selling legislation. Where the payee (e.g. a merchant) or its PSP fails to accept strong customer authentication, they are liable for the cost of the unauthorised transaction. (article 66(1))

- The right to compensation for liability attributable to another PSP has been supplemented to include compensation where a PSP fails to use strong customer authentication (article 82(2)).

**Liability: direct debits**

The payer is given an unconditional right to refund of a direct debit within eight weeks of the debit date, "except where the payee has already fulfilled the contractual obligations and the services have already been received or the goods have already been consumed by the payer" (article 67(1)). We assume the introduction of this statutory right is not intended to prevent PSPs from undertaking contractually to give better refund rights (as is currently the case for e.g. the UK direct debit scheme).

The new provision also adds the following: "At the payment service provider's request, the payee shall bear the burden to prove that the conditions referred to in the third subparagraph..." and ends there, i.e. with missing words. The intent is presumably to provide for refunds in every case unless the payee can prove that it has fulfilled its contractual obligations and the services have been received or goods consumed. (It is not clear however whether the intention is that the services must have been received in full to prevent refund.)

In addition to a full refund of the transaction, the credit value date on the payer's account must be treated as no later than the date the transaction was originally debited. We take this to mean that the interest on the account must be adjusted as if the transaction never took place.

**Access to TPPs**

Account servicing PSPs, who actually provide customers with an account and execute their transactions, will be required to allow their customers to give TPPs access to their accounts (article 58(1)). This will mean, for example, that banks will no longer be permitted to prohibit the use of account aggregation services in relation to their accounts (it remains to be seen how this will interact with other issues that affect aggregators, such as potential offences under the UK Computer Misuse Act). The purpose here, presumably, is to boost competition. However, it is likely to increase operational and legal risks for account servicing PSPs, with them having uncertain recourse against the TPPs in the event of TPP failures giving rise to, in particular, unauthorised transactions (see below).

Account servicing PSPs will also be required to allow their customers access to the services of a "third party payment instrument issuer" to obtain "payment card services" (article 59(1)). This is presumably intended to facilitate co-badging. However, there is some uncertainty as to scope, as neither "payment card services" nor "third party payment instrument issuer" is defined (is the latter intended to be a form of payment initiation service and/or the separate payment service of "issuing of payment instruments"?).

As further measures to ensure access to TPPs, the account servicing PSP is limited in its ability to inhibit or discriminate against payment orders transmitted through a payment initiation service provider or third party payment instrument issuer (articles 58(4), 59(3) and 61(2)), and is required to furnish them with information as to the availability of sufficient funds for a transaction to be made (articles 58(3) and 59(2)).

Account servicing PSPs and TPPs are likely to face operational challenges in engaging with each other to enable TPPs to deliver payment initiation and account information services. The account servicing PSP may need to put in place operational and IT measures to authenticate the status and identity of TPPs, feed account information to them, and accept instructions from them (see above and articles 58(2) and 87(2)). Some of these challenges will also apply where customers obtain payment card services from third party payment instrument providers, to the extent that they are not already acting as TPPs.

The provider of a payment initiation service needs to provide various transaction related information, both at the time of a transaction and in the event of fraud or a dispute, which in some cases will duplicate information provided by other PSPs (articles 38 to 40).

**Improper execution and unauthorised transactions involving TPPs**

Where payment initiation services are provided, and a transaction is improperly executed by the account servicing PSP, the onus is on the TPP to prove that it was not the cause of the improper execution (articles 64(1) and 80(1)).

TPPs are subject to security obligations (article 58(2)), including ensuring the inaccessibility of a customer's "personalised security features" and not storing their sensitive payment data or "personalised security credentials". Nonetheless, the account servicing PSP remains liable for unauthorised transactions even where a TPP is involved (articles 63 and 65).
There is, however, a reference to the possibility of a TPP providing financial compensation to the account servicing PSP (article 65(2)), but there are no operative provisions specifying when it would need to do so (albeit there is an indication of intent in recital (52): "a balanced liability repartition between the payment service provider servicing the account and the TPP involved in the transaction should compel them to take responsibility for the respective parts of the transaction that are under their control and clearly point to the responsible party in case of incidents").

Consequently, account servicing PSPs may be exposed to the cost of security breaches prompted by TPPs without having clear recourse against the TPPs to recover the losses (and even if there was recourse, a TPP might not have deep enough pockets to reimburse the cost of any systemic breaches that it has caused).

It is unclear why PSD2 leaves account servicing PSPs exposed in this way: possibly the Commission anticipates that in many cases TPPs will not have access to customers’ security credentials, such that they are not in a position to cause security breaches. However, we expect that TPPs would have such access at least where they are providing a payment instrument to the customer, or where they are providing account information services.

Complaints procedure

PSPs must put in place “adequate and effective” internal complaints resolution procedures, and provide related information (article 90). This includes having to respond fully to complaints in writing within 15 business days or, in exceptional circumstances, within a further 30 business days. This is likely to require changes to customer documentation and procedures (for example, the UK Financial Conduct Authority’s requirement for PSPs to respond to complaints within eight weeks will need to be shortened).

AGENTS, PASSPORTING AND SAFEGUARDING

Agents

There is a new specific requirement for PIs to inform their home State regulator of changes regarding the use of agents, including updating information provided by the PI when it originally registered an agent (article 18(9)).

Passporting

The EBA will issue:

- guidelines on when a PI should be passporting under the freedom to provide services or the freedom of establishment (article 26(5)); and
- draft standards (potentially to be adopted by the European Commission) for co-operation and exchange of information between home and host States in relation to a passporting PI and its passported agents (article 26(6)-(8)).

The EBA will need to issue the guidelines and draft standards within two years of PSD2 being adopted. It is hoped that they will result in a smoother and more harmonised process for passporting across the EU.

Safeguarding

PSD2 removes the current derogation (in article 9(4) PSD1) that allows individual member States to exclude from the scope of safeguarding any customers with funds of €600 or less.

INTERCHANGE REGULATION

Scope

The Interchange Regulation has greatest impact on "four party payment card schemes" meaning "a payment card scheme in which payments are made from the payment account of a cardholder to the payment account of a payee through the intermediation of the scheme, a payment card issuing payment services provider (on the card holder’s side) and an acquiring payment services provider (on the payee’s side), and card based transactions based on the same structure".

A "three party payment card scheme" is a "payment card scheme in which payments are made from a payment account held by the scheme on behalf of the cardholder to a payment account held by the scheme on behalf of the payee, and card based transactions based on the same structure”. However, the definition also provides that, "When a three party payment card scheme licenses other payment service providers for the issuance and/or the acquiring of payment cards, it is considered as a four party payment card scheme."

Despite acceptance on all sides that the current drafting of PSD1 is problematic for cards payments, no changes have been made to address that. Instead, PSD2 continues to assume that money is transferred from the cardholder to the merchant. For example, the words underlined in the above definitions are problematic for UK merchant acquirers’ “acquisition” model of acquiring. Given the uncertainty that this has created under PSD1, it would be a missed opportunity if PSD2
and the Interchange Regulation did not address these problems. This is likely to require strong industry engagement to explain to the Commission exactly how the payment schemes operate in practice.

CAPS ON INTERCHANGE FEES

Interchange fees for four party payment card schemes will be capped as follows.

From two months after publication of the Interchange Regulation, the maximum interchange fee for cross-border consumer debit and credit card transactions will be 0.2% and 0.3% respectively (article 3).

From two years after publication, the maximum interchange fee for all other consumer debit and credit card transactions will be capped at the same levels (article 4).

Transactions can be connected with multiple jurisdictions in different ways, and so PSPs will need to consider carefully the definition of what is or is not a cross-border transaction, in order to identify when the caps will start to apply in relation to particular transactions.

Circumvention of these rules is prohibited and interchange is defined as including all net compensation received by the issuer from the scheme (article 5). This may cause problems for revenue that is not historically associated with interchange such as contributions from schemes towards scheme-based marketing.

Caps on interchange fees (mainly for Visa and MasterCard payments) may drive card issuers to find alternative revenue streams, such as higher interest rates, or annual or monthly fees for cards.

REMOVAL OF CARD SCHEME RESTRICTIONS

The Interchange Regulation removes a number of restrictions that could otherwise impede competition:

Territorial limits – Scheme licenses for issuing or acquiring cannot be restricted to a specific territory but cover the entire EU (article 6).

Separation of schemes and processing - Schemes (other than three party schemes) and the entities which process card transactions must be separated to allow for competition and, to support this objective, territorial discrimination in processing rules is prohibited and technical interoperability of processing entities’ systems is required (article 7).

Co-badging and choice of application – issuers can decide whether a card or wallet is co-badged by one scheme or more and the consumer can choose which scheme to use when making payment (article 8).

Acquirers cannot blend merchant service charges but must charge retailers individually for different categories and different brands of payment cards and provide full information about those charges per category and brand (article 9).

Payment schemes and PSPs cannot require a retailer to 'Honour All Cards' i.e. accept a category or brand of card if he accepts another category or brand, unless the brand or category is subject to the same regulated interchange fee (article 10). For example, merchants accepting consumer debit cards may not be forced to accept consumer credit cards but can be required to accept other consumer debit cards.

Payment schemes and PSPs cannot prevent retailers from steering consumers towards the use of specific payment instruments preferred by the retailer or prevent retailers from informing consumers about interchange fees and merchant service charges (article 11). Limits on surcharges are contained in PSD2.

The removal of these restrictions may provide new opportunities for international issuing and acquiring businesses, which may in some way offset the loss of revenues that caps on interchange represent.

As a result of the changes, merchants will have greater control over the cards that they choose to accept, provided they do not discriminate between issuers of the same products, and will be able to surcharge where interchange fee caps do not apply, i.e. mainly Amex and other three party card schemes. This may lead to changes to consumer behaviour as they avoid expensive cards and may indirectly affect levels of merchant service charge on three party cards so as to ensure that they are as widely accepted as now.

The ability for issuers to co-badge their cards with links to more than one card scheme may lead to new and innovative products being created. In addition, measures facilitating TPPs’ access to the payments market under PSD2 mean that payment initiation services drawing on e.g. current accounts could be used in place of card transactions as another alternative payment method for customers to select when purchasing online.

TRANSPARENCY

PSPs will have to provide information about transactions to the merchant after the execution of an individual payment transaction or periodically (article 12). This is again designed to increase transparency and will require changes to merchant agreements.
Contacts

London:
Hogan Lovells International LLP
Atlantic House
Holborn Viaduct
London EC1A 2FG
Tel: +44 (0) 20 7296 2000

Jon Chertkow
Partner
Tel direct: +44 (0) 20 7296 2191
Email: jonathan.chertkow@hoganlovells.com

Julie Patient
Of Counsel
Tel direct: +44 (0) 20 7296 5790
Email: julie.patient@hoganlovells.com

Ben Regnard-Weinrabe
Partner
Tel direct: +44 (0) 20 7296 5649
Email: ben.regnardweinrabe@hoganlovells.com

Emily Reid
Partner
Tel direct: +44 (0) 20 7296 5362
Email: emily.reid@hoganlovells.com

Mark Taylor
Partner
Tel direct: +44 (0) 20 7296 5370
Email: mark.taylor@hoganlovells.com

Roger Tym
Partner
Tel direct: +44 (0) 20 7296 2470
Email: roger.tym@hoganlovells.com

Amsterdam:
Keizersgracht 555
1017 DR Amsterdam
Netherlands
Tel: +31 (20) 55 33 600

Victor de Vlaam
Partner
Tel direct: +31 (20) 55 33 665
Email: victor.devlaam@hoganlovells.com

Frankfurt:
Untermainanlage 1
60329 Frankfurt am Main
Germany
Tel: +49 (69) 962 36 0

Richard Reimer
Partner
Tel direct: +49 (69) 96236 414
Email: richard.reimer@hoganlovells.com

Madrid:
Paseo de la Castellana,
51 Planta 6º
28046 Madrid
Tel: +34 91 3498 200

Joaquin Ruiz Echauri
Partner
Tel direct: +34 (91) 3498 295
Email: joaquin.ruiz-echauri@hoganlovells.com

Paris:
17, avenue Matignon
Paris 75378
France
Tel: +33 (1) 53 67 47 47

Sebastien Gros
Partner
Tel direct: +33 (1) 5367 1623
Email: sebastien.gros@hoganlovells.com

Rome:
Piazza Venezia 11
Rome 00187
Italy
Tel: +39 (06) 675823 1

Jeffrey Greenbaum
Partner
Tel direct: +39 (06) 675823 28
Email: jeffrey.greenbaum@hoganlovells.com

Warsaw:
ul. Nowogrodzka 50
Warsaw 00695
Poland
Tel: +48 (22) 529 29 00

Beata Balas-Noszczyk
Partner
Tel direct: +48 (22) 5292 920
Hogan Lovells has offices in:

- Alicante
- Amsterdam
- Baltimore
- Beijing
- Berlin
- Brussels*
- Budapest*
- Caracas
- Colorado Springs
- Denver
- Dubai
- Dusseldorf
- Frankfurt
- Hamburg
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Jakarta*
- Jeddah*
- London
- Los Angeles
- Luxembourg
- Madrid
- Miami
- Milan
- Moscow
- Munich
- New York
- Northern Virginia
- Paris
- Philadelphia
- Prague
- Rio de Janeiro
- Riyadh*
- Rome
- San Francisco
- Shanghai
- Silicon Valley
- Singapore
- Tokyo
- Ulaanbaatar
- Warsaw
- Washington DC
- Zagreb*

*Hogan Lovells* or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses. The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www.hoganlovells.com.

©Hogan Lovells 2013. All rights reserved.

*Associated offices*