NEW PAYMENT SERVICES REGIME
PREPARING FOR A REVISED LANDSCAPE

Jon Chertkow, Julie Patient and Virginia Montgomery of Hogan Lovells explore how payment service providers should prepare for the implementation of the new directive on payment services.

The Payment Services Directive (*2007/64/EC*) (2007 Directive) started a massive programme of regulatory change for payments, which affected nearly all aspects of banking and payment service provision. It created a single market for payment services across the EEA, increased transparency, imposed uniform rules for execution times and eliminated non-transparent charges. The 2007 Directive was implemented in the UK by the Payment Services Regulations 2009 (*SI 2009/209*) (2009 Regulations) (*see feature article "Payment services regime: the nuts and bolts", www.practicallaw.com/5-501-4198*).

The Directive on payment services in the internal market (*2015/2366/EU*) (2015 Directive), also known as the second Payment Services Directive or PSD2, was published in the Official Journal of the EU on 23 December 2015. It will replace the 2007 Directive. With the exception of some requirements where the implementation period is linked to the finalisation of European Banking Authority (EBA) technical standards, EU member states will have until 13 January 2018 to implement the requirements of the 2015 Directive. Legally speaking, the UK's EU referendum result has no immediate effect as it is only advisory in nature. The UK continues to be a member of the EU today and, while the exact timing for the withdrawal process is still unclear, as things currently stand implementation programmes for the 2015 Directive will need to continue.

The changes being implemented through the 2015 Directive will have a significant impact on many in the payments industry: both the traditional providers and those taking advantage of the explosion in financial technology (fintech) opportunities to compete in the payments market alongside the traditional operators (*see box "Summary of key changes"*). The impact will be different depending on the type of payment service provider (PSP) and its range of services. For all, implementation will be challenging (*see Opinion "New payment services regime: a missed opportunity?", www.practicallaw.com/3-542-6685*).

The 2015 Directive builds on the requirements of the 2007 Directive. By tightening requirements in some areas, it addresses concerns that the 2007 Directive had not been implemented in the same way in all member states. More significantly, it makes changes designed to facilitate competition and innovation, and extends its scope to payments in non-EEA currencies and to payments where one of the PSPs is not in the EEA (a one leg out transaction).

As the countdown to implementation of the 2015 Directive begins, this article:

- Explains its increased scope.
- Looks at the introduction of two new payment services to cover the activity of so-called third-party payment service providers (TPPs) and therefore open a new market for innovators that want to use existing bank and payment infrastructures.
- Considers the major changes to the way that PSPs will be required to authenticate some payments.
- Outlines some further important changes from the current regime.
- Suggests some key action points for businesses currently subject to the regime and those that may come within the scope of the revised regime.

In this article, all references to legislation are to the 2015 Directive unless stated otherwise.

Summary of key changes

Key change	Impact
One leg out transactions and non-EEA currencies	• More onerous information and conduct requirements. • Changes to terms and conditions. • Changes to systems and processes. • Impact on charging arrangements.
Exemptions	• Less scope to rely on exemptions. • New authorisations required. • New business models may be needed.
New payment services	• New authorisations required. • Impact on account providers to allow for effective interaction.
Authentication	• New processes required. • Changes to terms and conditions. • Impact on payees, in particular retailers.
Reporting	• New processes required. • More robust systems and controls for some payment service providers.
Passporting	• Potentially more interference from host EU member state.
Complaints	• Shorter time periods to resolve complaints.

INCREASED SCOPE

The 2015 Directive expands the scope of the 2007 Directive by:

- Covering international and currency payments.
- Restricting the scope of some of the existing exemptions.
- Introducing new payment services.

One leg out and non-EEA currencies

Currently, the 2007 Directive only applies if:

- The PSPs of both the payer and the payee are within the EEA. One leg out transactions 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 the 2015 Directive, both limitations fall away and the 2015 Directive will apply, with some exceptions, to one leg out transactions in respect of those parts of the payment transaction which are carried out in the EU, and to payments 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 both previously excluded from the scope of the EU payment services regime (*see box "Action points on one leg out transactions and non-EEA currencies"*).

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 those customers are micro-enterprises), the changes will put one leg out and non-EEA currency payment transactions on an almost equal footing with EEA transactions.

Impact of increased scope

Key action points arising from this extension of scope under the 2015 Directive include:

Changes to terms and conditions. A large number of products and services, particularly US dollar and other currency accounts, were out of the scope of the 2007 Directive purely because they were in a foreign currency or were one leg out transactions. Those products will now need to be reviewed and their terms and conditions amended to comply with the 2015 Directive information requirements (*Title III*).

Changes to interest rates. The 2015 Directive (and the 2007 Directive) requires two months' notice of changes to contracts unless the change is an alteration to an interest rate that is linked to an external reference rate (*Article 54 (currently Article 44, 2007 Directive)*). 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 (*Article 59(2)*). In addition, explicit agreement will be needed to carry out a currency conversion (*Article 59(2)*).

Charges. "SHA" charging, where the payee and payer pay the charges levied by their own PSP, will be required for all payments within the EEA, even if there is a currency conversion (*Article 62(2)*). This will affect retail payments and transactions by large companies.

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

Action points on one leg out transactions and non-EEA currencies

In preparing for the implementation of the Directive on payment services in the internal market (*2015/2366/EU*), in relation to one leg out transactions and non-EEA currencies, payment service providers should:

- Identify the accounts and services that will be affected for the first time.
- Consider what changes will be needed to terms, and whether these are just cosmetic or will have a commercial impact.
- Establish the effect on operations.
- Ensure that they can provide the additional information required.
- Identify whether they need to change their interest or exchange rate basis.
- Consider whether they can apply the conduct provisions.
- Identify their reliance on correspondent banks.
- Consider whether the existing process allows for compliance, or whether new systems or processes are required.
- Consider whether any necessary changes will affect commercial arrangements.
- If they act as a correspondent bank, consider the effect on clients.
- Consider whether their services are compliant and, if not, what changes need to be made.

originated (*Article 87*). This impact is limited to large corporate accounts as other accounts were already subject to a similar rule under the Financial Conduct Authority's (FCA) Banking Conduct of Business sourcebook (BCOBS).

Correspondent banking. Many of the above changes are likely to require amendments to current correspondent banking arrangements and practices, and could affect the commercial pricing of these arrangements.

Exemptions

Many of the exemptions in the 2007 Directive will be retained. Cheques and other paper-based transactions will remain outside of scope, as will inter-bank and other settlement transactions. However, a number of exemptions have been clarified to ensure that they are applied on a consistent basis across member states. The changes will particularly affect non-bank institutions that currently rely extensively on some of these exclusions, such as mobile network operators. The following three key exemptions will be less useful going forward:

Digital download exemption. This will be restricted to mobile network operators and 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 (*Article 3(l)*).

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" (*Article 3(k)*). In addition, the FCA must be notified if the total value of transactions in any 12-month period exceeds €1 million (*Article 37(2)*). This creates a proactive duty on the FCA to check that the PSP is right to rely on the exemption.

Commercial agent exemption. The commercial agent exemption has been relied on by a number of payment intermediaries, particularly in the download market. It will be restricted to payment transactions through a commercial agent that is authorised to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee (*Article 3(b)*). Just acting as an intermediary with no real ability to negotiate will not be sufficient.

Businesses that currently rely on these exemptions will need to decide whether they can continue to operate outside of the payment services regime (*see box "Action points on exemptions"*). Some will need to apply for authorisation as payment institutions while 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 the payment services regime as a result of these restrictions on the current use of exemptions.

INTRODUCTION OF TPPS

When the 2007 Directive was implemented, there was much debate about the banking services that fell within its scope. It is now settled that the following banking products, in particular, are payment services:

- Current accounts (including associated facilities such as debit cards), flexible savings accounts generally and e-money accounts.
- Credit cards and other forms of revolving credit that can be used to make payments.
- Certain "one accounts", which combine mortgage, savings and payment functionality.
- Cash withdrawals at ATMs.
- Merchant acquisition services.
- Money transfer or money transmission services.

New payment services

The 2015 Directive attempts to deal with the pace of payments innovation by introducing two new payment services to cover the activity of TPPs: payment initiation services and account information services.

A payment initiation service 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 (*Annex 1*). This is intended to cover services such as SOFORT in Germany and iDEAL in the Netherlands, which enable a customer to use a payment gateway to log in directly to their bank account in order to make an online purchase.

An account information service is an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSP (*Annex 1*). This will cover account aggregation services, which provide consumers with a consolidated

view of their bank accounts and enable them to access their accounts online.

2015 Directive and TPPs

The 2015 Directive attempts to do two things in relation to TPPs: to bring them within the scope of regulation and to promote competition by facilitating their operation.

Payment initiation services and account information services are already provided in a number of member states, often on an unregulated basis. The first objective of the 2015 Directive is to ensure that they are brought within the scope of regulation. In order to provide one of these services, a business will need to become authorised as a payment institution if it is not already permitted to carry on payment services (*Articles 2(1), 4(15)-(16), 5; Annex I*).

The second objective is to make it easier for these TPPs to operate by mandating how the account servicing PSPs must interact with them. This area will be of particular concern for existing PSPs and is likely to be a major focus of PSPs' implementation projects, although there is some crossover with other initiatives such as the UK Open Banking Working Group's activities relating to its Open Banking Standard framework on the creation, sharing and use of open banking data (*https://theodi.org/open-banking-standard*).

Although there are a number of account information service providers operating in the UK, whether payment initiation service providers will disrupt the UK payments market remains to be seen. With the UK acting as a major hub for fintech, further innovation in this area is likely with both new entrants and the traditional PSPs exploring whether these services can provide new income streams or ways to improve customer retention.

Account services and TPPs. PSPs providing payment accounts that are accessible online will be required to allow their customers to give TPPs access to their accounts (*Article 36*) (*see box "Action points on access by TPPs"*). 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 effects. For example:

- Payment initiation service providers that provide card-based instruments will need to be given information about the availability of funds for a transaction.
- Data requests from an account information service provider will need to 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 (*Title II, Chapter 2; Title IV*).

In addition, ensuring that the right PSP bears the cost of improper execution and unauthorised transactions involving TPPs will be challenging because:

- The PSP providing the payment account is primarily liable to the customer.
- The burden is on the TPP to prove authentication of the payment but only within its "sphere of competence".
- The PSP providing the payment account can seek to recover from the TPP but may have no direct contractual relationship.
- To protect against credit risk, TPPs will be required to have insurance but there are questions as to whether this will be available and, in circumstances where there is a major security breach, whether it will be sufficient (*Article 5(2)-(3)*).

At this stage, it is difficult to predict whether TPPs will cause market disruption. The fact that the traditional providers will have to facilitate the TPP services in a marketplace where they will be competing for the same customers, and income streams, will no doubt cause some concerns. It remains to be seen whether these new service providers will be able to develop products that are attractive to consumers and establish consumer confidence sufficient to transform the payments market.

Action points on exemptions

If a payment service provider currently relies on any of the exemptions in the Payment Services Directive (*2007/64/EC*), in order to comply with the Directive on payment services in the internal market (*2015/2366/EU*), it will need to:

- Assess whether its business still falls within the scope of the relevant exemption; for example, by considering what range of goods can be bought and whether that range is really "very limited".
- Become authorised if the business clearly no longer falls under the exemption. There are no transitional arrangements so work on becoming authorised will need to start straight away.
- If authorisation is not an option, think about how its service can be changed in order to fall within the exemption; for example, by partnering with an authorised institution.

SECURITY

Security is another key focus of the 2015 Directive 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) will have to use "strong customer authentication" when a payer:

- Accesses a payment account online.
- Initiates an electronic payment transaction.
- Carries out any action through a remote channel that may imply a risk of payment fraud or other abuses (*Article 97(1)*).

In addition, where a payment is initiated electronically, elements of the strong authentication must be "dynamically linked" to a specific amount and a specific payee (*Article 97(2)*).

Strong customer authentication means authentication based on the use of two or more elements categorised as knowledge, possession and inherence that are

independent (*Article 4(30)*). That means the breach of one should not compromise the reliability of the others.

If a payer's PSP does not require strong customer authentication, the payer will only be liable for a disputed transaction where it is committing fraud. If the payee's PSP does not accept strong customer authentication, that PSP will be liable for any unauthorised transaction, in a similar way to the current liability model for 3D Secure transactions (a fraud prevention scheme for online credit and debit card transactions).

EBA technical standards. The EBA will work with the European Central Bank 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.

The 2015 Directive reflects the strong customer authentication requirements already in place through the European Forum on the Security of Retail Payments (SecuRe Pay) recommendations and EBA guidelines on internet payment security, which have already been adopted in a large number of member states. However, the drafting style of the EBA technical standards should be 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, the provisions on security, including the strong customer authentication requirements, in Articles 65, 66, 67 and 97 of the 2015 Directive will not come into force until 18 months after the technical standards are finalised.

In December 2015, the EBA issued a discussion paper with the aim of obtaining early input into the development of the draft technical standards relating to strong customer authentication and secure communication under the 2015 Directive (*www.eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf*). In the discussion paper, there is an acknowledgement that it will not always be necessary or convenient to request the same level of security from all payment transactions and that exemptions to the principle of strong customer authentication will be possible. These exemptions will be defined by the EBA based on the risk involved, the value of transactions and the channels used for payment.

While a definitive set of exemptions has not yet been provided, the EBA suggests that the following exemptions could apply:

- Low-value payments, as defined in the 2015 Directive, provided that the risks for cumulative transactions are monitored.
- Outgoing payments to trusted beneficiaries included in previously established white lists by a payment service user.
- Transfers between two accounts of the same payment service user held at the same PSP.
- Low-risk transactions based on a transaction risk analysis.
- Purely consultative services, with no display of sensitive payment data, taking into account data privacy laws.

The EBA also confirmed that exemptions for all payments made through a certain channel cannot be justified. The EBA intends to issue a consultation on the draft technical standards in summer 2016.

Impact of strong customer authentication. All PSPs, including TPPs, will need to ensure that they comply with the new strong customer authentication requirements for all of the potential types of payments within scope. It will not be 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 that currently use PINsentry-type mechanisms to access online banking, that is, devices that generate unique codes to keep online banking transactions secure. Within the UK, solutions are being considered in a number of sectors but PSPs that provide account services will need to put in place systems that allow a TPP to rely on their authentication method.

Retailers may be concerned that a customer's checkout 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 on strong customer authentication, although many retailers will hope that the EBA's technical standards will provide flexibility where they have robust fraud controls in place.

Action points on access by TPPs

The Directive on payment services in the internal market (*2015/2366/EU*) raises a number of issues in relation to access by third-party payment service providers (TPPs):

- Potentially huge operational changes are required for banks and others to ensure that they can allow access to TPPs.
- The industry needs to engage with the European Banking Authority 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 payment service providers.
- Wide-ranging analysis will need to be undertaken to ensure that payment service providers 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 has not already begun.

Reporting requirements

Applicants to be a new payment institution will have to provide additional information. 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 the illegal use of data (*Article 5(1)(j)*) (*see box "Action points on security"*).

As well as considering the reporting requirements under the proposed Directive concerning measures to ensure a high common level of network and information security across the EU (NIS Directive) and the General Data Protection Regulation (*2016/679/EU*), all PSPs will need to report major operational or security incidents to the FCA (*Article 96*) (*see Briefing "General Data Protection Regulation: preparing for change", www.practicallaw.com/5-626-9787*). If a security incident might affect the financial interests of customers, the PSP must also directly notify affected customers without undue delay and inform them of measures that they can adopt to mitigate the adverse effects (*Article 96(1)*). The EBA will issue guidelines to help PSPs determine when they need to report security incidents.

There will be 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 these risks (*Article 95(2)*).

Impact of reporting requirements

FCA-regulated firms are already required to provide details of their security arrangements but the new requirements will provide a structure for all PSPs. Reporting issues to the FCA (and, for banks, to the Prudential Regulation Authority) will become standard practice for all PSPs.

Of more concern may be the requirement to inform customers of security incidents "without undue delay" as companies might become more likely to revert to the media in a similar way to TalkTalk's decision to warn its customers that their personal data, including bank details, were at risk following cyber attacks on its website in 2015. In the initial communication, TalkTalk announced that it did not know how many customers were affected, which led to concerns that many of its four million customers could be at risk. This early announcement, which was made before TalkTalk had obtained all relevant information on the extent of the security breach, had a serious effect on its reputation. In fact, 156,959 people (4% of its total number of customers) had been affected.

Action points on security

In preparing for the implementation of the Directive on payment services in the internal market (*2015/2366/EU*), in relation to security, payment service providers should:

- Identify where strong customer authentication is not currently used and how it can be implemented. If it cannot be implemented, payment services providers will need to consider whether the service should be withdrawn
- Identify areas for engagement with the European Banking Authority 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 they can evidence effectively that these arrangements are fit for purpose.

OTHER CHANGES

The 2015 Directive will bring about a number of other changes. Not all of them are set out in this article but some further important changes are outlined below.

Passporting for payment institutions

To address concerns over the effectiveness of the current passporting regime for payment institutions, the 2015 Directive 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 or the freedom to provide services must provide the home member state with information about their operations (*Article 28(1)*). The home member state must then send this information to the competent authorities of the host member state within one month (*Article 28(2)*). This is the same requirement that currently applies under Article 25 of the 2007 Directive.

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 (*Article 28(2)*). If the home member state disagrees with the assessment, it must provide the host member state with reasons for its decision (*Article 28(2)*). Overall, the home member state has three months from the receipt of information from the payment institution to communicate its decision to both the host member state and the payment institution (*Article 28(3)*).

The host member state can require payment institutions that have agents or branches within that member state to report to it periodically (*Article 29(2)*). 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 (*Article 29(4)*). 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 that a payment institution with agents or branches in its territory is non-compliant, it must inform the home member state without delay (*Article 30(1)*).

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 (*Article 30(2)*). 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.

In December 2015, the EBA consulted on draft technical standards on passporting for payment institutions (*www.eba.europa.eu/documents/10180/1306972/EBA+CP+2015+25+%28CP+on+RTS+on+Passporting+Notifications%29.pdf*). Final form technical standards are due to be published in summer 2016.

Complaints procedure

PSPs will have to put in place adequate and effective internal complaints resolution procedures, and provide related information (*Article 101(1)*). 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 that clearly indicates the reasons for the delay and specifies a deadline by which the PSP will respond fully to the complaint (*Article 101(2)*).

The deadline for the final written response cannot be more than 35 business days after receipt of the complaint (*Article 101(2)*). This is likely to require changes to customer documents and procedures. The current requirement is for PSPs to respond to complaints within eight weeks.

Merchant acquiring

The 2007 Directive has always regulated merchant acquiring but, because it erroneously treated card transactions as similar to direct debits, there has been considerable uncertainty as to how the requirements applied.

The 2015 Directive introduces a new broad definition of merchant acquiring which should assist in identifying whether those that provide point of sale payments solutions outside of the traditional card acquiring models are caught by the requirements (*Article 4(3); Annex I*). Unfortunately, the 2015 Directive has not taken the opportunity to clarify exactly how card acquiring operates and how the requirements are intended to apply, so continued uncertainty is expected in this respect.

NEXT STEPS

The timetable for implementation is challenging. With the 2007 Directive, the Treasury finalised the regulations nine months before the implementation deadline and the then regulator, the Financial Services Authority, published its draft approach document seven months before that date. Implementation programmes had to be well underway before the 2007 Directive and approach document were finalised, requiring firms to make massive investments on the basis of assumptions about how the 2007 Directive would be implemented.

A similar approach is expected here but with the added complexity of the 2015 Directive leaving much of the detail of certain requirements to EBA technical standards. At the time of writing, the Treasury has not yet consulted on the implementation of the 2015 Directive but is expected to begin consultations in summer 2016. The FCA has recently sought views on its current approach document and anticipates that it will consult further over the next two years to focus on the changes brought about by the 2015 Directive (*www.fca.org.uk/static/fca/documents/call-for-input-payment-services-regime.pdf*).

As with any implementation project, when businesses start to focus on the practical issues of implementation, further questions will emerge. With new providers entering the market and the changes to scope, we anticipate that implementing the 2015 Directive will be equally as challenging as implementing the 2007 Directive.

Depending on when the government makes the notification of its withdrawal from the EU under Article 50 of the Treaty on the European Union, and assuming that no extension of the two-year withdrawal period is granted, the UK could potentially leave the EU soon after the implementation deadline for the 2015 Directive. Work to shape the future of the UK payment services regime will present both challenges and opportunities but, in the meantime, the implementation deadline edges ever closer.

Jon Chertkow is a partner, Julie Patient is counsel, and Virginia Montgomery is a senior professional support lawyer, at Hogan Lovells.

Related information

This article is at practicallaw.com/8-630-5425

Other links from practicallaw.com/

Topics

Banking	topic7-385-1287
Payment services	topic9-103-2034
Regulation: finance	topic4-103-1094

Practice notes

Hot topics: PSD2	2-554-0865
Payment Services Regulations 2009: background, scope and key terms	8-519-8105
Payment Services Regulations 2009: FCA supervisory approach	4-519-9927
Payment Services Regulations 2009: information requirements that payment service providers must comply with under Part 5	3-519-8179
Payment Services Regulations 2009: rights and obligations of customers and payment service providers under Part 6	5-519-9781
UK implementation of the Payment Services Directive	5-381-9528

Previous articles

Mobile payments: financial services and digital businesses converge (2013)	9-528-6286
Payment services regime: the nuts and bolts (2010)	5-501-4198
Payment Services Directive: ready for the new regime? (2009)	0-500-5686

For subscription enquiries to Practical Law web materials please call +44 207 202 1200