

Client Alert

13 November 2014

Progress on Payment Services in Europe

By Simon Deane-Johns, Ombria Poindexter, and Alistair Maughan

The European Union is in the process of updating its regulatory regime for payment services to reflect the developing nature of the payment services market. The European Commission's proposed revised Payment Services Directive ("PSD2") will cover a wide range of payments-related services and businesses. But questions remain about the scope and effect of the European regulatory regime that PSD2 does not fully answer.

This Alert discusses the most recent changes in the EU's proposals, and explains the key differences between PSD2 and the current EU payment services regime.

The first EU Payment Services Directive ("PSD") was adopted in 2007 and became law in most EU member states in 2009. In July 2013, the European Commission published its proposal for PSD2, which was the subject of an earlier [Alert](#). The proposal was updated on 12 September 2014 by the Council of the European Union and twice again in October 2014, and this Alert reflects the latest proposal. If and when PSD2 is finally adopted, member states will have two years to implement its provisions into their national laws. However, further amendments may be made during the EU parliamentary process.

In its current form, PSD2 will impact payment institutions, e-money institutions and their agents and technology providers. But it will also affect:

- existing or proposed investors in payment institutions and e-money institutions;
- operators of e-commerce marketplaces, gift card and loyalty programs;
- bill payment services providers;
- public communication network operators;
- payment initiation services providers;
- account access services providers; and
- digital wallet providers.

The original PSD was implemented in order to open the EU markets for regulated payment services to new entrants, both by creating a new form of regulated financial institution ("payment institution") and endorsing certain unregulated activities through specific exemptions. Importantly, the PSD substantially reduced the initial capital required to enter the regulated market. The first Electronic Money Directive ("EMD1"), introduced in 2000, required electronic money institutions ("EMIs") to hold initial capital of €1m. But in 2009, the PSD enabled payment institutions to launch other types of payment services with only €125,000 of initial capital. In 2011,

Client Alert

EMD2 reduced the initial capital for EMI's to €350,000. As a result, there are now over 200 EU-regulated payment institutions, 80% of which are based in the UK (as are the majority of e-money institutions).

TERRITORIAL SCOPE

PSD2 is intended to apply to "payment services provided within the Union". The main provisions that apply to the provision of payment services are those requiring disclosure of certain information to customers and customer contracts (Title III) and creating specific rights and obligations (Title IV). These main provisions are to apply:

1. to payment transactions in the currency of a member state, where both the payer's and payee's payment service providers ("PSPs") are located "therein";
2. with a few exceptions, to payment transactions not in the currency of a member state, where both the payer's and payee's PSPs are located "therein" in relation to the parts of the payment transaction carried out in the EU;
3. with many exceptions, to payment transactions where only one of the PSPs is located "within the Union, in respect to those parts of the payment transaction which are carried out in the Union."

Unfortunately, it is not clear whether the word "therein" in the first two provisions refers to the member state or anywhere in the EU. So, it is not clear whether the PSP must be located in the member state specifically or the EU generally. As a result, in adopting PSD2, each member state may choose to ignore the specified exceptions in each case, thereby opening up the possibility of inconsistent assertions of jurisdiction throughout the EU (see "Passporting" below). In addition, the definition of "direct debit" as "a national or cross-border payment service..." raises possible scope issues where the relevant border is between a member state and a non-member state, or between two non-member states.

Payment institutions (and e-money institutions) will have to carry out at least part of their business in their home member states in order to qualify for authorisation by the local regulatory authority.

BILL PAYMENT SERVICES

Bill payment services enable a consumer to pay, for example, a utility bill on the basis that payment to the service provider discharges the customer's obligation to pay the supplier. The UK's Financial Conduct Authority, for example, considers these services to be out-of-scope of the PSD because the supplier who issued the bill is not the intended recipient of funds. However, the recitals to PSD2 direct EU member states to treat bill payment services as money remittance unless the activity falls under another payment service. This tension between legal reality and perceived consumer intent also surfaces in the inconsistent treatment of e-commerce platforms and public communications networks (discussed below), creating considerable uncertainty in the application of both the PSD and PSD2.

PAYMENTS ANCILLARY TO A CORE BUSINESS ACTIVITY

In the recitals to PSD2, the European Commission suggests that e-commerce platforms (undefined) have unfairly relied on being the agent of both consumer and merchant, rather than of one or the other, to remain outside the scope of the PSD (often called the "commercial agents exemption"). Accordingly, the exemption has been

Client Alert

amended to allow the agent to be authorised to negotiate or conclude the sale or purchase of goods or services on behalf of both the payer and the payee only if the agent does not enter into possession of either payment service user's funds.

Somewhat inconsistently, the PSD also has an exemption for transactions involving the purchase of digital content on a telecommunication network "as ancillary services to electronic communications services" (*i.e.*, the core business of the operator concerned). PSD2 limits this exemption to €50 per transaction and either a total of €200 per billing month or, in the case of pre-funded accounts, €200 per calendar month. However, the exemption will apply regardless of the device used for the purchase or consumption of the content. The term "digital content" is perhaps unintentionally limited by the qualification that the content must "not allow in any way the use or the consumption of physical goods or services". For example, a software application (including a mobile app) could be said to "allow the use" of the physical device on which it runs.

In addition, member states may allow an exemption for payment transactions of up to €10 each, or €100 a month in total, "by a provider of electronic communication networks or services for a subscriber" where those transactions are performed from or via an electronic device and charged to the related service bill for either the purchase of tickets or "within the framework of charitable activity". The notes to PSD2 suggest that the ticket exemption is limited to tickets related to transport, but this is not clear from the exemption itself. Firms relying on either exemption will need to notify their local regulator of such activities and provide an annual auditor's report testifying that they meet the requirements for the relevant exemption.

TECHNOLOGY SERVICE PROVIDERS

The PSD exempts services provided by technical service providers that support the provision of payment services without the service provider entering into possession of the funds to be transferred. However, PSD2 provides that such services will be exempt only if they are offered to PSPs rather than to payment services users. The notes to PSD2 state that this is intended to cover so-called "gateway" services such as transaction data transfer services which are often supplied to merchants in parallel with a card acquiring service, rather than to the acquirer.

LIMITED NETWORKS

The PSD currently exempts payment transactions based on payment instruments accepted only within the issuer's premises or certain limited networks. This applies to "closed loop" stored value cards and other instruments such as retail store cards, gift cards, fuel cards and loyalty programmes. Such instruments are also exempt from the definition of "electronic money" in the second electronic money directive ("EMD2") by reference to the PSD exemption.

This exemption survives under PSD2 and has been extended to cover public instruments for specific social or tax purposes. However, it is now explicit that the same instrument cannot be used in more than one limited network or to acquire an "unlimited range of goods and services". As to what is meant by "unlimited", the recitals to PSD2 state that "instruments which can be used for purchases in stores of listed merchants should not be exempted... as such instruments are typically designed for a network of service providers which is continuously growing."

Client Alert

Limited network operators will also be obliged to notify the regulator if "the average of the preceding 12 months' total value of payment transactions executed exceeds €1million". It seems implicit that this must be an average of €1million transactions per month. The regulator must then inform the European Banking Authority ("EBA"), which will add the firm to a public list of such operators. This process will clearly give regulators the opportunity to disagree that the limited network exemption applies. That will be a concern in relation to cross-border programmes involving member states whose regulators interpret either the threshold or the application of this exemption differently.

Where a regulator decides that a service does not qualify for the limited network exemption, there is no provision for an orderly transition to enable the operator to either obtain full authorisation or become the registered agent of an authorised payment institution or e-money institution to continue operating the service.

AUTOMATED TELLER MACHINE (ATM) SERVICES

PSD2 maintains the exemption for services which enable the withdrawal of cash from ATMs where the service provider is acting on behalf of card issuer(s) who have no contract with the cardholder. But exempt ATM service providers cannot offer any other regulated payment services, and must give the cardholder and the payee certain information about each transaction before and after processing.

THIRD PARTY PSPs

PSD2 introduces various types of "third-party" PSPs (referred to here as "TPPs"). These are entities that offer only the new "payment initiation services" or "account information services", or that engage in the slightly revised service of "issuing payment instruments". TPPs may be contrasted with "account servicing payment service provider[s]" ("ASPs") who provide and maintain payment accounts from which payers want specific transactions to be made.

The new "payment initiation service" is a "service to initiate a payment order at the request of a payment services user with respect to a payment account at another service provider". Member states must ensure that payers have the right to use a payment initiation service in relation to payment accounts that are accessible online. A firm offering such a service will be called a "payment initiation service provider". Such firms must not handle the payer's funds in connection with the provision of the payment initiation service.

The new "account information service" is a service to provide consolidated information on one or more payment accounts held by a payment service user with one or more other PSPs. The provider of such a service is an "account information service provider". While such firms will be exempt from certain authorisation requirements, they will be treated as payment institutions and will be able to "passport" throughout the EEA, for example. However, they will not need to comply with the information and contractual requirements in Titles III and IV, with certain exceptions.

The existing PSD service of "issuing of payment instruments" is now defined as "a payment service where a payment service provider provides the payer with a payment instrument to initiate **and** process the payer's payment transactions" (emphasis added). This distinction is presumably to differentiate this activity from a "payment initiation service".

Client Alert

The information that PSD2 requires to be provided to customers also seems to broaden the concept of "payment instrument". Where customers are shown a range of different card-scheme brands as payment options prior to checkout (called "co-badging"), they should be informed that they have the right to select a particular brand and to change their selection at point of sale. This stage in the checkout process is itself referred to as "the issuance of a payment instrument", as opposed to the payment methods shown as available, and suggests that the entity that serves up this part of the checkout process is itself the issuer of a payment instrument and should be authorised accordingly. It is likely that many e-commerce merchants will host their own checkout page or process, in which case the transaction moves to the acquirer's servers only once the customer has selected which type of payment instrument she wishes to use or (if the merchant is PCI compliant) once the transaction is captured and sent to the acquirer. So, this new requirement could effectively require merchants either to cease hosting any aspect of the checkout process or to become authorised as payment issuers or agents of firms so authorised.

TPPs that provide payment initiation will need initial capital of €50,000 and (along with account information service providers) must hold professional indemnity insurance. TPPs are also subject to the full weight of the information and contractual requirements and various obligations in Title IV, except where a member state exempts account information service providers from such requirements.

Any TPP that initiates payment transactions carries the burden of proving that within its "sphere of competence" the payment transactions were authenticated, accurately recorded and not affected by a technical breakdown or other deficiencies linked to "the payment service it is in charge of".

As well as providing certain data about the transactions initiated through them to the payer, TPPs must also provide such data to the payee. It is not clear how that could be achieved, given that there is usually no direct relationship between each payment service user and the other user's PSP. It seems more likely that the TPP initiating the transaction will be in a position to transmit data only to the payer's ASP and the payee's ASP.

ACQUIRING SERVICES

In PSD2, the term "acquiring of payment transactions" is defined as "a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which result in a transfer of funds to the payee." Leaving aside the circularity in the definition, it is not clear from whom the transfer of funds to the payee must originate. Consistent with the re-casting of the "technology service provider" exemption, it would seem that a supplier of technology services under an agreement with the payee, as opposed to the PSP (e.g., "gateway" data transfer services supplied to a merchant) would be covered by this definition, even though the service provider does not enter into possession of any funds due to the payee.

ACQUISITIONS OF SHARES IN PAYMENT INSTITUTIONS

Under PSD2, the existing or proposed shareholder, rather than the payment institution or e-money institution, will have the obligation to inform the authorities of any decision to acquire or increase a shareholding in that institution. The authorities will be empowered to oppose or block such acquisitions in certain circumstances.

Client Alert

SECURITY AND USE OF PAYMENT ACCOUNT DATA

The initial version of PSD2 contained relatively high-level security requirements. It mandated the use of "strong customer authentication", as well as additional internal controls related to security and fraud and proposed risk management and incident reporting obligations for PSPs.

However, the latest version of PSD2 is far more prescriptive. Member states may reduce the €50 limit of liability where a payer has not fraudulently or intentionally failed to either keep security credentials "safe" or notify the service provider of loss, theft, unauthorised use, etc., of a payment instrument.

PSD2 now contains specific authentication and data handling rules relating to TPPs depending on whether they initiate payments, issue a payment instrument or provide account information services; and different rules for ASPs in their dealings with different types of TPPs.

ASPs may discriminate against data requests through account information service providers only where objectively justified. However, ASPs can agree with payment service users to deny access to payment account data for any TPPs "for objectively justified and duly evidenced reasons related to unauthorised or fraudulent use of payment initiation services"; but the ASP must inform the payer and unblock the access once the reason no longer exists.

Subject to exemptions in EBA technical standards to be developed in due course (see below), all PSPs must apply strong authentication when a payer accesses a payment account online; initiates an electronic payment transaction; and/or "carries out any action through a remote channel which may imply a risk of fraud or other abuses". In the case of an electronic payment transaction that is initiated via the Internet or "other at-a-distance channel" (a "remote payment transaction"), the authentication must "include elements dynamically linking the transaction to a specific amount and a specific payee".

PSD2 also establishes breach notification requirements for PSPs. Specifically, all PSPs must establish an operational risk management framework and provide the regulator with their assessment of the risks and the adequacy of their controls. In addition, PSPs must classify "major incidents", which must be reported to their home state authority without undue delay. In turn, the home state authority must report such major incidents to the EBA and the European Central Bank. Where a security incident (one assumes a major security incident) impacts the financial interests of users, the PSP must, without undue delay, inform the users of the incident and the possible measures that users can take to mitigate adverse effects.

EBA TECHNICAL STANDARDS

PSD2 empowers the EBA to set various technical standards, including those for strong customer authentication and communications among PSPs and with users. These standards may allow exemptions based on the level of risk; the amount or recurrence of a transaction; and "the payment channel used to execute the transaction". Initial drafts of these technical standards should be available 12 months before the time for implementation of PSD2 at the national level, and the EBA is currently consulting on certain guidelines. But there is no explicit deadline for such guidelines to be finalised, while PSPs will be obliged to implement the standards within 30 months after PSD2 takes effect. The EBA is tasked also with reviewing and, if appropriate, updating the standards "on a regular basis", but the frequency of such reviews is not specified.

Client Alert

SURCHARGING

PSD2 bans surcharging for the use of payment cards and any other instruments in relation to which interchange fees are separately regulated. Member States may also ban or limit surcharging for their own domestic card-based transactions (*i.e.*, where the issuer, acquirer and point of sale are in the same Member State).

REFUNDS FOR PAYMENT TRANSACTIONS

PSD2 provides that where any unauthorised payment transaction was initiated through a payment initiation service provider other than the provider of the relevant payment account, the payer can obtain a refund from either PSP. If the refund is paid by the "innocent" PSP, it can obtain compensation from the "guilty" PSP for the reasonable costs incurred, in addition to the amount of the refund. The same rights apply in the case of non-executed or defective payment transactions.

A payer is to be entitled to a refund of authorised payment transactions initiated by or through a payee (*e.g.*, direct debits) if the authorisation did not specify the exact amount of the payment when authorised and the amount "exceeded the amount the payer could reasonably have expected[,] taking into account the previous spending pattern, the conditions in the framework contract and relevant circumstances of the case". Here the onus is on the payer to prove that the conditions are met, but PSPs can agree to refund direct debits (in particular), even if the above conditions are not met. Equally, the PSP can agree that there is no right to a refund for a transaction initiated by or through a payee where consent was given directly to the PSP and, where applicable, information on the transaction was provided to the payer by the PSP or payee at least 4 weeks before the due date.

However, regardless of the refund position, a payer can *revoke* a payment order for a direct debit by the end of the business day before the due date for debiting the funds (and later if agreed with the PSPs).

FRAMEWORK CONTRACTS

As under the PSD, a PSP will be able to agree with users that they are deemed to have accepted changes to their contracts if they do not object within the two months' notice of those changes taking effect. However, under PSD2, the PSP must also inform the users that they have the right to terminate the contract free of charge with effect from the date when the changes would have applied. PSD2 will involve various changes to existing agreements for the ongoing supply of payment services.

FORCE MAJEURE

Typically, force majeure arises where a party is prevented from performing an obligation due to circumstances beyond that party's "reasonable control". However, Article 83 refers to consequences "which would have been unavoidable despite *all efforts* to the contrary, or where a [PSP] is bound by other legal obligations covered by national or Union legislation". This arguably introduces a best-efforts type obligation.

COMPLAINTS HANDLING

The overall deadline for a firm to resolve a complaint is reduced from 8 weeks to 15 business days (or up to a total of 45 business days if there is a delay for reasons beyond the control of the PSP, and the PSP indicates the reasons for delay and the date for a final reply). This significantly accelerates the deadline for referrals to the Financial Ombudsman Service (in the UK), for which payment service providers pay a substantial fee.

Client Alert

PAYMENTS MADE BY MISTAKE

If a payer makes a payment to the wrong payee through the payer's own error, the payer's PSP must make reasonable efforts to recover the funds involved. The payee's PSP must also cooperate in these efforts and, where a payee refuses to give up the funds, the payee's PSP must inform the payer of the payee's identity and address, with notice to the payee. This would enable the payer to commence proceedings for restitution, etc., of the funds paid by mistake, if necessary.

PASSPORTING

PSD2 will stipulate a revised process for payment institutions and e-money institutions to exercise their rights to offer their services in other member states on either a branch basis (within 60 days), or cross-border service basis (within 40 days).

However, host states are also empowered to require passporting firms operating through branches or agents under the right of establishment to report to them on the activities carried out in the host territory by the firm's agents or branches. Host states may then contact the passporting firm's home state authority with any allegations of non-compliance thereby appearing to create a process by which a host state could escalate any differences in its interpretation of PSD2 with the home state. Such action could undermine the concept of home state control that is especially important for consistency in services provided using agents who refer electronic transactions across borders (e.g., e-commerce aggregators), rather than transactions that originate via physical branches or stores.

NON-DISCRIMINATORY ACCESS TO BANK ACCOUNTS

Credit institutions (banks) will not be permitted to discriminate in the provision of bank account services to authorised or registered payment institutions or e-money institutions.

TRANSITIONAL ARRANGEMENTS

Transitional provisions will give existing payment institutions an extra 6 months from implementation at the national level to obtain any additional authorisation(s) required under PSD2. While PSD2 nominally requires payment institutions to provide information that enables the regulator to assess whether such payers still meet all the conditions for authorisation, member states may give their regulators power to grant authorisation automatically where they already have such information.

E-money institutions will also have an extra 6 months to provide the authorities with the information to grant them fresh authorisation. However, there seems to be no opportunity for member states to allow regulators to do that automatically based on evidence already available to them.

Firms operating under a waiver would have an extra 12 months either to become authorised or to obtain a fresh waiver, unless the regulator has enough evidence to automatically grant the waiver where that power is given.

Failure to satisfy the regulator's conditions for authorisation or a waiver would mean that the firm is no longer authorised, or the waiver is lost, as the case may be.

Client Alert

Contact:

Obrea O. Poindexter
(202) 887 8741
opoindexter@mofo.com

Alistair Maughan
+44 (0)20 7920 4066
amaughan@mofo.com

Simon Deane-Johns
+44 (0)7539 848 096
sdeanejohns@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's* A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.