Client Alert

February 1, 2016

FinTech Focus: New European Directive on Payment Services (PSD2) Comes into Force

By Simon Deane-Johns and Susan McLean

On 12 January 2016, the long-awaited revised Payment Services Directive ("PSD2") came into force in Europe. This replaces the Payment Services Directive ("PSD") that has been in place since 2007. The deadline for EU member states to implement PSD2 into their national laws and regulations is 13 January 2018.

PSD2 is a significant reform to the EU regulatory regime for payment services and has been introduced to take into account significant innovations in card, internet and mobile payment services since 2007, and to better reflect the current (increasingly crowded) European payment services market. Crucially, it covers a wider range of payments-related services and businesses than PSD and will require providers to change their systems and processes to comply with the new rules.

Given its potential impact, it's surprising how little mainstream coverage PSD2 has received. In addition, questions remain about the scope and effect of the European regulatory regime for mobile payments that PSD2 doesn't fully answer. As with the PSD that it replaces, PSD2 is not entirely consistent with the contractual, operational or technical reality of how some payment methods operate.

In this Alert, we summarise some of the key differences between PSD2 and the existing PSD regime.

WHO IS AFFECTED BY THE NEW DIRECTIVE?

PSD2 impacts existing payment service providers (such as banks, payment institutions and e-money institutions ("PSPs")) and their agents and technology providers (and investors), as well as the operators of e-commerce marketplaces, gift card and loyalty programmes, bill payment services, public communication networks, payment initiation services, account access services and digital wallet services.

Territorial scope

PSD2 has a broader scope than PSD, which was limited to payments within the EU. PSD2 applies (with certain exceptions) to payment transactions carried out in the EU: (a) in a non-EU currency, where both PSPs are located in the EU; and (b) in any currency, where only one of the PSPs is located within the EU, (sometimes referred to as "*one leg out transactions*"). This is considered an important improvement for consumers, particularly in the area of global money remittance. A PSP will have to carry out at least part of its business in its home member state in order to qualify for authorisation by the local regulator.

Exclusions/exemptions: PSD provided a list of specific 'exemptions', plus a 'waiver' of certain provisions to be granted by the authorities in certain instances. PSD2 calls the specific exemptions 'exclusions'; and the activities

that may currently be waived 'exemptions'. For the purposes of this Alert, we use the term "exemption" to refer to activities that are specifically excluded from scope; and "waiver" to refer to activities the authorities decide won't be subject to the regulations.

Bill payment services: Historically, opinions have differed among member states and the Commission as to whether services that enables a consumer to pay a bill to an intermediary, rather than the supplier (*e.g.*, utility bills) fall within the scope of the PSD. The UK regulator, the FCA, for example, considered these services out-of-scope of the PSD because the supplier issuing the bill is not the intended recipient of funds. However, the recitals to PSD2 make clear that bill payment services should be treated 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 telecoms networks (discussed below), creating uncertainty in the application of PSD2 and its overall market impact.

Commercial agents: In the recitals to PSD2, it is stated that the commercial agents' exemption has been applied very differently across EU. It is suggested 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. Accordingly, in PSD2, the exclusion has been amended so that it only applies if the commercial agent is authorised to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee. Where agents act on behalf of both payer *and* payee, they should be excluded only if they do not at any time enter into possession or control of client funds.

Electronic communications networks/service providers: Under PSD2, only digital content or voice-based services provided via an electronic device as an ancillary service and charged to the related telecoms bill are excluded. Digital content means goods or service produced and supplied in digital form whose use or consumption is restricted to a technical device and does not include the use or the consumption of physical goods or services content (*i.e.,* apps, wallpaper, ringtones, videos, games etc.) PSD2 also excludes services performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets. These exclusions are aimed at micro-payments with a low risk profile. Accordingly, PSD2 limits both of these exclusions to €50 per transaction and either a total of €300 per month or, in the case of pre-funded accounts, €300 per month, for each subscriber.

Limited networks: The PSD exempts payment transactions based on payment instruments accepted only within the issuer's premises or certain limited networks, or used to only acquire a "limited range" of goods or services. The E-money Directive also applies this 'limited network exemption' to exclude "closed loop" stored value cards and instruments such as retail store cards, gift cards, fuel cards and loyalty programmes. Under PSD2, the limited network exclusion is extended to cover public instruments for specific social or tax purposes. However, it's now explicit that the same instrument can only be used to acquire a "very limited range of goods and services". As to what is meant by "very limited", the recitals to PSD2 gives guidance that instruments that can be used for purchases in stores of listed merchants should not be excluded "as such instruments are typically designed for a network of service providers which is continuously growing".

Limited network operators must notify the regulator if the total value of transactions executed over the preceding 12 months exceeds €1million. The regulator will then decide whether the exclusion criteria apply and will notify

the operator if it concludes they do not. That will be a concern in relation to cross-border programmes involving member states whose regulators interpret the application of this exclusion differently. Where a regulator decides that a service doesn't qualify for the exclusion, there's no provision for a transition period (*e.g.*, to allow the operator to either obtain full authorisation or become the registered agent of a PSP to continue operating the service; or for an authorised PSP to become the operator (by transfer or otherwise); or for the orderly winding down of the affected scheme).

Third Party Payment Services: There have been many new entrants into the payment services market since 2007. These include 'third party' PSPs (referred to here as "TPPs") who offer payment initiation and account access or aggregation services. Until now, these TPP have faced significant barriers to offering their solutions across the EU because of security and secrecy concerns raised by some PSPs.

PSD2 addresses these concerns by bringing TPPs within scope and splitting them into three categories: (i) PSPs that offer payment initiation services, (ii) PSPs that offer account information services and (iii) by altering the definition of issuing payment instruments. TPPs may be contrasted with "account servicing payment service provider" ("ASPs"), who provide and maintain payment accounts for a consumer.

- *Payment Initiation Services*. These services involve initiating a payment order at the request of a user with respect to an account held with another PSP, without handling the funds. Unfortunately, there are differing opinions as to how certain types of payments are initiated and who is the "payee" or "intended recipient of funds", especially in relation to card-based payments. PSD2 provides that consumers must have the right to use a payment initiation service in relation to their online payment accounts (whether or not there is any contractual arrangement in place between the PSP and the payer's ASP).

  TPPs who provide only payment initiation services will need initial capital of €50,000 and hold professional indemnity insurance or "some other comparable guarantee" against their regulatory liabilities. These TPPs are also subject to the full weight of the information and contractual requirements and obligations to contribute to losses arising from those parts of the transaction under their control, except where a member state exempts account information service providers from such requirements. However, these TPPs will not have to meet any additional 'own funds' requirements.

- *Account Information Services*. These are online services which provide consolidated information from a user's payment account(s), (typically to enable the user to have an overview of their finances and analyse their finances). PSD2 provides that consumers must have the right to use such a service whether or not there is any contractual arrangement in place between the account information service provider ("AISP") and the user's ASP.

  While AISPs will be exempt from authorisation under PSD2, they will need to be registered. They will be treated as payment institutions and will be able to passport throughout the EEA. They will need to hold professional indemnity insurance or a comparable guarantee and comply with certain information and contractual requirements under PSD2.

These arrangements are backed by a separate PSD2 requirement that banks permit PSPs access to their payment account information (*i.e.*, via open APIs) on an "objective, non-discriminatory and proportionate basis", where they have the explicit consent of the user. Such access must be "extensive enough" to allow PSPs to provide payment services "in an unhindered and efficient manner". Banks are also required to provide their regulator with "duly motivated reasons for any rejection". Many have seen this as a significant step towards more open banking that will benefit consumers and new providers alike.

- *Issuing of Payment Instruments.* Issuing of payment instruments services are redefined under PSD2 to be "payment service(s) by a payment service provider contracting to provide a payer with a payment instrument to initiate *and* process the payer's payment transactions". This is presumably to distinguish this activity from a 'payment initiation service'.

  The information that PSD2 requires to be provided to users also seems to broaden the concept of "payment instrument". Where users are shown two or more payment brands or payment applications of the same payment brand on the same payment instrument (called "co-badging"), they must be informed of their various rights under the Merchant Interchange Fees Regulation. However, there is no reference to the ban on multilateral interchange fees or equivalent charges for direct debits (except certain problem transactions on certain conditions) under the Single European Payment Area (SEPA) Regulation.

  Showing customers a range of payment options would typically be done at the end of a 'checkout' process. PSD2 refers to this stage in a checkout process itself as "the issuance of a payment instrument", as opposed to each of the available payment methods. This 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's likely that many e-commerce merchants currently host their own checkout page or process, in which case the transaction only moves to the acquirer's servers either once the user has selected which type of payment instrument he/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 to either cease hosting any aspect of the checkout process, or become authorised as payment issuers or agents of firms authorised to issue payment instruments.

ATM services: PSD2 also contains an exclusion for services that enable cash withdrawal from ATMs where the service provider is acting on behalf of card issuer(s) who have no contract with the cardholder. However, excluded ATM service providers can't offer any other regulated payment services, and must give the cardholder and the payee certain information about each transaction before and after processing.

Technology service providers: PSD2 makes clear that the exclusion for technology service providers will not apply to TPPs.

Passporting: PSD2 sets out a revised process for PSPs to exercise their rights to offer services in other member states on either a branch basis (within 60 days), or cross-border service basis (within 40 days). Banks will passport under a separate, but similar regime. However, host states also have the power to require passporting firms to appoint a central point of contact. Host states can contact the passporting firm's home state regulator with any allegations of non-compliance. This could enable a host state to escalate any differences in its

interpretation of PSD2 to the home state regulator, which could undermine the concept of home state control that is especially important for consistency in services provided using agents who refer electronic transactions across borders (*e.g.*, e-commerce 'aggregators').

Security and use of data: PSD2 introduces the concept of "strong customer authentication", as well as additional internal security and fraud controls and risk management and incident reporting obligations. Subject to any exemptions found in European Banking Authority (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. 'Strong customer authentication' means authentication based on the use of two or more independent elements that are based on something only the user knows (knowledge), something only the user possesses (possession) or something the user is (inherence), as well as designed to protect the confidentiality of the authentication data.

PSPs must adopt specific security requirements to protect the confidentiality and integrity of the users' personalised security credentials. The ASP must allow TPPs to rely on the authentication procedures provided by the ASP to the user of both services. For payment transactions initiated via the internet or through a device that can be used for distance communications, the authentication must include elements that dynamically link the transaction to a specific amount and a specific payee.

PSD2 also establishes incident notification requirements for PSPs. In particular, PSPs must establish an operational risk management framework and provide the regulator with an assessment of the risks and the adequacy of their controls. In addition, PSPs must classify "major operational and security incidents", that must be reported to their home state regulator without undue delay. Where a major operational or security incident has, or may have, an impact on the financial interests of its users, the PSP must, without undue delay, inform those users of the incident and "all available" measures they can take to mitigate the adverse effects of the incident.

EBA security and technical standards: PSD2 empowers the EBA to set various technical standards, including for strong customer authentication and communications. An initial set of standards took effect in 1 August 2015 in most member states, although the FCA has said that it cannot apply them to UK-based PSPs until PSD2 has been implemented locally.

Consumer Protection

- *Charges*. Users will only be liable for transaction charges where the full amount is disclosed to them before the initiation of the transaction.
- *Surcharges*. PSD2 bans surcharges for the use of payment cards (and any other instruments in relation to which interchange fees are separately regulated).
- *Statements*. Payers must be given a contractual right to ask for at least monthly transaction statements, free of charge. Member states can require PSPs to extend this right to payees.

- *Contracts*. PSPs can continue to agree with users that they are deemed to have accepted contract changes if they don't object within two months of being notified of those changes taking effect. However, under PSD2, the PSP must also inform users that they have the right to terminate the contract free of charge with effect from the date the changes would have applied. PSD2 also requires that termination of a framework contract must be free of charge for the user after the contract has been in force for 6 months. In other circumstances, any charges for terminating a framework contract must be appropriate and in line with costs.

- *Complaints*. Under PSD2, the deadline for resolving complaints is reduced from 8 weeks to 15 business days (or, up to 35 business days if there is a delay for reasons beyond the PSP's control, and the PSP indicates the reasons for delay and the date for a final reply). Member states can, however, provide for faster redress. PSPs must have complaints resolution procedures that apply in every member state where the PSP offers payment services, in the official language of the member state or in another language if agreed between the PSP and the user. The Commission will produce a leaflet explaining user's rights, and PSPs will have to make the leaflet available via their websites and on paper in physical locations.

Liability

- Under PSD2, the amount for which a user can be held liable is reduced from 150€ to 50€. Member states may reduce this €50 limit of liability where a payer has not fraudulently or intentionally failed to either keep security credentials "safe" or notify the provider of loss, theft or unauthorised use of a payment instrument.

- PSPs will bear the burden of proving a payment transaction was authorised, and will need to provide evidence of any alleged fraud or gross negligence on the part of the user, rather than relying on the fact that the payment instrument was used successfully.

- In addition, PSD2 provides that where an 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 the TPP or the ASP. 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 refund. The same rights apply in the case of non-executed or defective payment transactions. To avoid a refund obligation, the payer's PSP must communicate to the local authorities its grounds for suspecting fraud. A payer is entitled to a refund of authorised payment transactions initiated by or through a payee (*e.g.*, direct debits) if the authorisation didn't 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 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 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 involved).

- If a payer makes a payment to the wrong payee in error, the payer's PSP must make reasonable efforts to recover the funds. The payee's PSP must also cooperate by communicating to the payer's PSP all relevant information. Where a payee refuses to give up the funds, the payer's PSP must give the payer, upon written request, all relevant information available to it in order for the payer to file a legal claim to re-collect the funds. It is not clear whether the payee's identity and address is within the scope of "all relevant information".

Acquisitions of shares in payment institutions: Under PSD2, the existing or proposed shareholder, rather than the PSP, will have the obligation to inform the authorities of any decision to acquire or increase a shareholding in that institution. The authorities can oppose or block such acquisitions in certain circumstances.

Transitional arrangements: Transitional provisions give existing PSPs an extra 6 months from implementation at the national level to obtain any additional authorisation(s) required. While PSD2 nominally requires existing payment institutions to provide information that enables the regulator to assess whether they still meet *all* of the authorisation conditions, member states can give their regulators power to grant authorisation automatically where the regulator already has such information. However, there doesn't appear to be the same opportunity to grant automatic authorisations in the case of existing e-money institutions. Firms operating under a waiver have 12 months from when PSD2 takes effect to become authorised or obtain a fresh exemption, unless the regulator has enough evidence to automatically grant the exemption. Failure to satisfy the regulator of the conditions for authorisation or an exemption would mean the firm is no longer authorised, or the exemption is lost.

CONCLUSION

The growth in Europe's FinTech sector shows no sign of letting up, with a steady stream of new entrants creating products and services that challenge traditional payment business models and practices.

Even prior to the arrival of PSD2, there was recognition that the sector needed to change in order to compete with the services provided by the new FinTech operators (and/or acquire or partner with them). Indeed, a 2015 survey of over 100 banks carried out by Finextra identified that 54% of all respondents agreed or completely agreed that they were in the process of rethinking their retail banking customer relationship and revenue/business model.

Now that PSD2 has been adopted, the banks have an additional driver for that change programme.

Contact:

Simon Deane-Johns
44 (75) 39848096
sdeanejohns@mofo.com

Susan McLean
44 (20) 79204045
smclean@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 12 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.