PSD2 IMPLEMENTATION: WHAT YOU NEED TO KNOW

With just a few months to go, PSD2 brings with it a number of implementation challenges, not least in relation to the new regime for third party payment service providers, or TPPs. This briefing sets out what firms implementing the new requirements need to know.

Key issues

- National implementation deadline 13 January 2018
- UK implementation via the Payment Services Regulations 2017
- RTS on SCA and CSC not yet finalised; likely to apply from mid-2019
- Key changes include:
  - Expansion of scope
  - Regulation of TPPs
  - Changes to refund and liability rules
  - New cybersecurity regime
  - New complaints handling and dispute resolution rules
- Payment institutions to become re-authorised or re-registered

PSD2 AT A GLANCE

The revised Payment Services Directive (PSD2) overhauls the existing EU framework for the regulation of payment services under the original Payment Services Directive (PSD1). It broadens the scope of payment services regulation in the EU and brings third party payment service providers (TPPs) within scope of regulation for the first time. It also introduces changes to conduct of business requirements aimed at improving consumer protection and competition and changes to security and transparency requirements.

It is the result of a number of drivers, including the need to catch up with technology developments, a desire to increase competition in the payments market and facilitate new fintech businesses to provide payment services as well as react to the increased threat of cyber attack. The need to strike a balance between these sometimes competing aims of innovation, competition and security has been a common theme throughout the development of PSD2, most notably in relation to the regulation of TPPs and the development of regulatory technical standards that will govern their ability to access payment accounts and data held with banks and other account providers (ASPSPs).

Timing

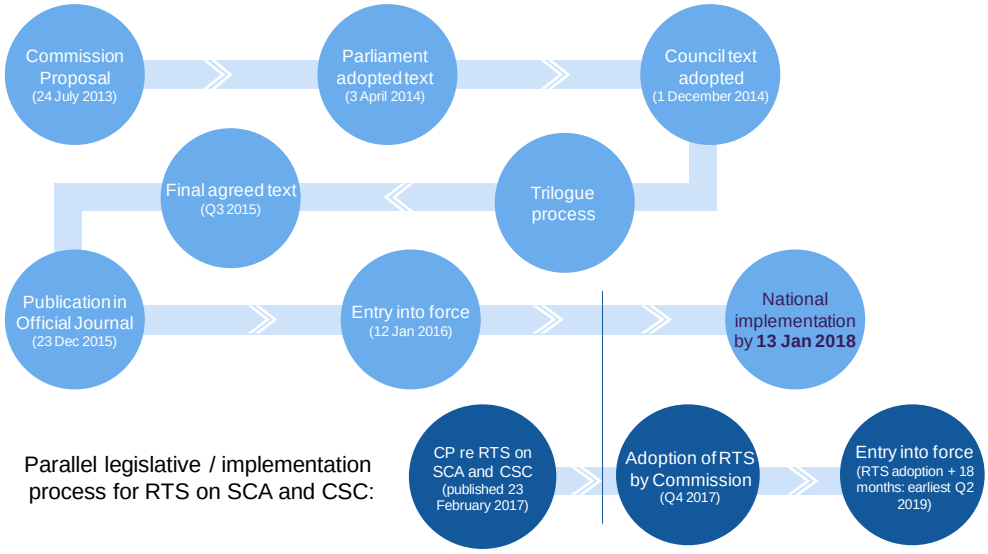
PSD2 entered into force on 12 January 2016 and must be transposed into Member States' national laws and regulations by 13 January 2018. Therefore, payment service providers (PSPs) will need to promptly assess the potential impact of PSD2 on their business and, if they have not done so already, swiftly take the steps necessary to implement any resulting changes to documentation, systems and processes by 13 January 2018.

RTS and guidelines

PSD2 empowers the European Banking Authority (EBA) to draft regulatory technical standards (RTS) and guidelines, including RTS on strong customer authentication (SCA) and secure communication (CSC), guidelines on authorisation and registration under PSD2, guidelines on security measures for operational and security risks, guidelines on major incident reporting and guidelines on fraud reporting requirements.

Work on many of these measures is ongoing and in some cases, firms may have only a short implementation timeframe after they are finalised. For example, the EBA is currently consulting on its fraud reporting requirements guidelines and has not yet published final guidelines on security measures for operational and security risks, although both sets of guidelines are expected to apply from 13 January 2018. On the other hand, whilst the RTS on SCA and CSC are not yet finalised, they are expected to apply 18 months after publication in the Official Journal.

PSD2 development and implementation timeline



UK implementation

As PSD2 is a Directive, it is not directly applicable but instead needs to be implemented into national law by the law-making bodies of each Member State. In the UK, PSD2 will be transposed into national law primarily through the Payment Services Regulations 2017 (PSRs 2017), which will repeal and replace the existing Payment Services Regulations 2009.

The Financial Conduct Authority (FCA) will continue to be the UK regulator responsible for authorisation and supervision of PSPs under PSD2. It has consulted on proposed changes to its rules and guidance, and has published a draft of its revised approach document setting out the FCA's role and supervisory approach under both the PSRs 2017 and the current Electronic Money Regulations 2011. This includes proposals to require existing authorised or registered payment institutions to submit applications for re-authorisation or re-registration under the PSRs 2017, subject to a transitional period. The Payment Systems Regulator is also responsible for certain aspects of PSD2 relating to regulation of payment systems.

However, the FCA has not yet published final Handbook changes or its final approach document and so firms may have only a short period between publication of the FCA's final rules and guidance and application of relevant requirements from 13 January 2018. In the absence of finalised rules and guidance, firms will need to use consultation drafts as a basis for developing their preparations and executing their implementation plans.

Firms are likely to encounter similar timing issues in other Member States. As at September 2017, only around half of Member States had published national implementing legislation and rules, and delayed implementation seems likely

in a handful of jurisdictions. Sweden has even confirmed that it will not implement PSD2 until May 2018 (in line with the General Data Protection Regulation (GDPR) coming into force).

See "*Implementation and next steps*" below for further detail about implementation issues, including the options and discretions granted to Member States under PSD2.

INCREASED SCOPE

Non-EU currencies and one-leg out

PSD2 brings more transactions and currency accounts into scope. Transactions in non-EU currencies will now be caught, as will "one-leg out" payment transactions, where only one PSP is located in the EU, "in respect of those parts of the payment transaction which are carried out in the Union".

As a result, more conduct of business and information requirements will apply to international payments. Firms should therefore consider whether any changes to systems, controls or client documentation may be needed to comply with these requirements particularly for accounts or agreements that previously fell outside the scope of PSD1. For example, firms may decide to include "corporate opt-out" language in agreements with corporate clients, in respect of accounts now within scope.

The limitation of PSD2 requirements to those parts of a payment transaction that are carried out in the EU aims to address the concern that PSPs may not have control over, or be able to fulfil their obligations in respect of, the parts of a transaction taking place outside of the EU. This may be because aspects of the transaction are subject to foreign payment systems and rules, for example. PSPs will therefore need to assess which parts of each transaction qualify as having been "carried out in the Union". In the absence of guidance as to the precise meaning of this wording, this may not be a straightforward exercise.

Narrowing of exclusions

Various existing exclusions under PSD1 have been narrowed or clarified, including the exclusions for ATM operators, commercial agents, use of payment instruments within a limited network and electronic communication network providers.

As a result, some firms that were previously able to rely upon an exclusion under PSD1 may no longer be able to do so under PSD2, and so they may need to become authorised or registered under PSD2 from 13 January 2018. PSD2 also introduces notification requirements for firms seeking to rely on the limited network exclusion or the electronic communication network exclusion, as summarised below.

ATM operator exclusion (Article 3(o))

The exclusion for ATM operators has been retained in PSD2 but ATM operators will be subject to new obligations to provide customers with information on withdrawal charges, both prior to the transaction and on the customer's receipt, with the aim of enhancing transparency.

Commercial agent exclusion (Article 3(b))

The commercial agent exclusion applies to commercial agents who negotiate or conclude the sale and purchase of goods and services on behalf of a payer or payee. The drafting of this exclusion has been amended to address Member States' divergent implementation of this exclusion under PSD1.

PSD2 clarifies that the commercial agent exclusion applies when the agent acts only on behalf of either the payer or only on behalf of the payee (and not both). However, Recital (11) of PSD2 provides that agents acting on behalf of both parties (such as in the case of some e-commerce platforms) may still be excluded, but only if the agent does not come into possession or have control of clients' funds.

Limited network exclusion (Article 3(k))

Under PSD2, the limited network exclusion applies to services based on payment instruments that may be used only within a limited network of service providers, to acquire a very limited range of goods or services, or where the payment instrument is regulated by a public authority for specific social or tax purposes to acquire specific goods or services. Payment instruments covered by the limited network exclusion would typically include shopping centre gift cards, fuel cards for a specific fuel network or employer dining cards or vouchers.

PSD2 amends the existing limited network exclusion to address concerns that it was being interpreted too broadly, and that firms were relying upon in it when providing payment instruments that could be used in multiple limited networks to purchase a wide range of goods and services. PSD2 therefore provides that it will not be possible to use the same payment instrument within more than one limited network and narrows one limb of the exclusion so that it relates to instruments used to acquire a "very" limited range of goods and services (rather than a "limited range" under PSD1).

PSPs seeking to rely on the limited network exclusion will also have to notify their national regulator and provide a description of their activities, if the value of transactions executed through the limited network exceeds €1 million in a 12 month period. The regulator must then decide if these services fall within the limited network exclusion and notify the firm if it concludes the services do not fall within the exclusion. The regulator also has an obligation to notify the European Banking Authority (EBA) of services that do fall within the limited network exclusion.

National regulators and the EBA will include the identity of PSPs relying on the limited network exclusion, together with a description of their activities falling within the exclusion, in the public registers of payment service providers that they are required to maintain under PSD2.

In the UK, firms will need to notify the FCA that they intend to rely on the limited network exclusion, if the value of payment transactions exceeds €1 million in the previous 12 months. The FCA has indicated that these firms must continue to provide notifications annually, unless their transaction value for the previous year falls below the €1 million limit.

Electronic communications network exclusion (Article 3(l))

PSD2 replaces the existing mobile device content exclusion with an exclusion for transactions carried out by a provider of an electronic communication network for ticket purchases or charity donations that are carried out from or via an electronic device, or for purchase of digital content or voice-based services (e.g. ringtones, music and premium SMS-services), in each case where the transaction is charged to the subscriber's bill. PSD2 introduces quantitative caps on this exclusion, of EUR 50 per transaction and EUR 300 per month.

That is not the end of the story, however, and firms seeking to rely on the exclusion must notify and provide to their national regulator (i.e. the FCA for UK firms) a description of the service and an annual audit opinion that their customers' transactions fall within the financial limits provided for in the exclusion.

As with the limited network exclusion, the national regulator must notify the EBA of services falling within this exclusion (or notify the firm if it concludes that the firm cannot rely on the exclusion) and firms relying on the electronic communications network exclusion will appear in the national and EBA public registers of payment service providers, together with a description of their activities falling within the exclusion.

THIRD PARTY PAYMENT SERVICE PROVIDERS

The provisions in PSD2 relating to TPPs, in particular the requirements for providers of online payment accounts to allow TPPs access to their customers' accounts, have sparked intense debate about where to strike the balance between opening up the payments market to fintechs and maintaining appropriate security standards for online payments and data; a debate that is heavily influenced by banks' risk aversion in the context of the new GDPR.

Broadly, TPPs provide payment services in respect of payment accounts that are accessible online and that the payment service user (PSU) holds with another PSP (the account servicing PSP, or ASPSP). TPPs may provide:

- payment initiation services (PIS), to initiate payments from a payment account the PSU holds with an ASPSP; and/or
- account information services (AIS), to provide the PSU with consolidated information about payment accounts it holds with one or more ASPSPs,

which are both new payment services being introduced under PSD2. Therefore, firms providing PIS and/or AIS may need to become authorised or registered for the first time under PSD2.

In the UK, the FCA has indicated it will also require credit institutions to notify it if they will be carrying on PIS and/or AIS, even though they will not be subject to any separate authorisation or registration requirements. Therefore, banks will need to assess whether they are already carrying on either or both of these new payment services and if so, submit a notification to the FCA.

Authorisation / registration requirements for TPPs

TPPs providing PIS must become authorised as payment institutions under the PSRs 2017 (unless authorised as a credit institution or an electronic money institution (EMI)).

A TPP that only provides AIS may become a "registered account information service provider" (RAISP) instead of becoming authorised under the PSRs 2017. RAISPs are subject to a lighter regulatory regime than authorised payment institutions. For example, they are not subject to any minimum capital requirements.

Article 5 PSD2 outlines the information that firms must provide as part of their application for authorisation as a payment institution (or registration as a RAISP). The EBA has also published guidelines setting out further detail about the information that these firms must provide.

Article 5 PSD2 also requires TPPs seeking authorisation as a payment institution or registration as a RAISP to hold appropriate professional

TPP applications for authorisation or registration

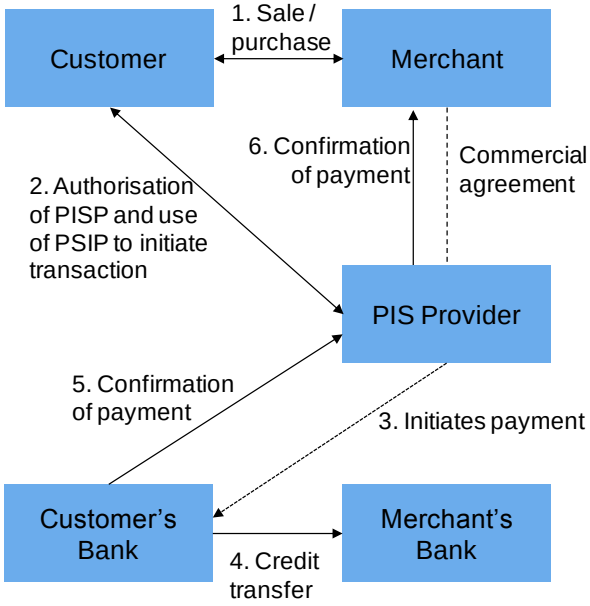
TPPs applying for authorisation as a PI or registration as a RAISP must provide information including:

- a programme of operations and business plan;
- evidence that the TPP holds the required level of initial capital (€50,000 for PIS and €0 for RAISPs);
- evidence of professional indemnity insurance held;
- information about the applicant's structural organisation;
- governance arrangements and internal control mechanisms;
- information about directors and other individuals responsible for the management of payment services;
- business continuity arrangements;
- security policy document;
- procedures for incident reporting; and
- processes relating to protection of sensitive payment data.

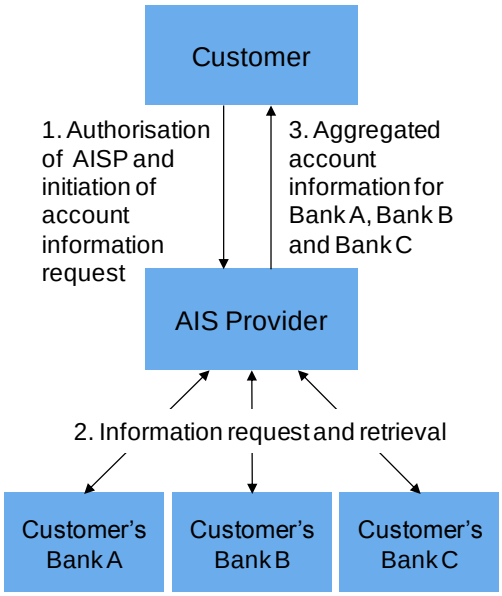
indemnity insurance (PII) or a comparable guarantee. HM Treasury has acknowledged concerns that suitable PII may not be available, and is engaging with TPPs and insurers on this issue.

In the UK, firms will be able to apply to the FCA to become authorised or registered as TPPs under the PSRs 2017 from 13 October 2017.

Payment initiation services: basic structure



Account information services: basic structure



Scope of PIS and AIS

Much of the initial discussion about bringing PIS and AIS within scope of regulation focused on services provided to consumers. For example, Recital (29) PSD2 explains that PIS offers a "*low-cost solution for both merchants and consumers and provide consumers with a possibility to shop online even if they do not possess payment cards*".

However, the definitions of PIS and AIS at Article 4 PSD2 are clear that they are not limited to a retail context nor are they subject to the corporate opt-out, and in its consultation on implementation of PSD2 and subsequent response, HM Treasury made it clear that the UK government reads these definitions broadly.

In response to industry concerns that these definitions might capture corporate treasury functions, price comparison websites, or services provided by accountants, financial advisors or legal firms via third party mandates (TPMs), HM Treasury commented that it does not intend to expressly carve out such TPMs from the definition of PIS and AIS, but that many uses of TPMs are likely to be outside the scope of PSD2. It gives the example of a power of attorney "*where the services are unlikely to be undertaken 'in the course of business*'".

Where a firm does have a TPM over a bank account, it will need to assess whether it may be providing PIS and/or AIS, or whether the service falls outside scope of PSD2, for example because it is not undertaken 'in the course of business'. This may not be a straightforward exercise and HM Treasury advises that "*[t]he FCA will assess individual business models on a case-by-case basis, and the government encourages firms to engage with the FCA if they think that their business model could fall within the regulatory perimeter*".

Implications for ASPSPs

Access to payment accounts

PSD2 seeks to ensure that ASPSPs do not undermine the business offerings of TPPs, by requiring ASPSPs to allow TPPs providing PIS or AIS access to online payment accounts (with the customer's consent) in order to initiate payment transactions or request relevant account information.

PSD2 requires a TPP to authenticate itself towards the ASPSP and communicate securely with the ASPSP. However, PSD2 prohibits ASPSPs from requiring TPPs to enter into contracts with them as a condition for allowing such access, although banks may wish to consider incentivising TPPs to enter into contractual arrangements.

ASPSPs can only discriminate against TPP-initiated transactions or information requests for objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account, and must allow access again once the reasons for access denial no longer exist. Where an ASPSP denies access to a TPP it must also report this to the PSU and to its national regulator. Therefore, ASPSPs should consider the parameters they would use when deciding whether to reject or delay TPP-initiated transactions or information requests.

The EBA has drafted RTS covering how TPPs should be able to access payment accounts, including how TPPs should communicate with and authenticate themselves towards ASPSPs. These RTS have been subject to much debate and have not yet been published in the Official Journal. See "*The TPP access debate*" below for further detail.

TPPs: implications for ASPSPs

- Mandatory right for PSUs to use TPPs
- ASPSPs must allow TPPs access to accounts to provide PIS and AIS
- No corporate opt-out
- New liability waterfall for transactions involving TPPs
- Prohibition on mandatory contract as a condition of access for TPPs
- Reporting requirements for access refusal

The TPP access debate

Currently, TPPs typically gain access to clients' payment account information by having clients share their login details with the TPP. Under this model, the

TPP effectively impersonates the client when logging in and obtains payment account information by "screen scraping".

However, access based on screen scraping is difficult to square with the new security requirements imposed under PSD2, which require ASPSPs to ensure that TPPs identify themselves securely, can access only the data necessary to provide a given service to their customers, and that the relevant customer has consented to this access. Banks worry, quite rightly, of the risk of fraudsters getting access to customer bank accounts and/or personal data security breaches.

This data protection concern is particularly acute given that the GDPR will apply from May 2018, bringing with it potential monetary penalties for breach of its requirements of up to €20 million or 4% of annual global turnover.

On the other hand, PSD2 establishes the right of PSUs to use TPPs in a bid to increase competition in the payment market, and fintechs see access to accounts as an opportunity to establish a profitable business model for payments without having to establish and maintain costly bank account infrastructure.

Development of the RTS on SCA and secure communication

These competing objectives of security and competition have shaped the development of the RTS on SCA and CSC, which set out the manner in which TPPs will be able to access payment accounts under PSD2, including how they should communicate with and authenticate themselves towards ASPSPs.

The EBA published its final draft RTS in February 2017. In this final report the EBA expressed its view that that screen scraping should no longer be allowed once the RTS start to apply, in light of the requirements in PSD2 regarding TPP identification, secure communication and the limitations on TPPs' access to data. Instead, the RTS required ASPSPs to offer at least one interface for TPPs to access payment account information. This may be the same interface as offered to and used by their customers (e.g. online banking) or, crucially, ASPSPs may opt to provide a separate, dedicated interface for use by TPPs – in other words, access based on an application programming interface (API).

The EBA attempted to address TPPs' concerns about their ability to access payment accounts where a dedicated TPP interface does not work properly, by requiring ASPSPs to provide the same level of availability and performance, including contingency measures in case of unplanned unavailability, as the interface offered to and used by their customers.

On 4 May 2017, around 60 fintech companies wrote to EU policymakers and national legislators, arguing that the EBA's attempts to address TPP access concerns did not go far enough and setting out their concerns that banks would have too much control over their business models and that the proposed RTS would adversely impact innovation, competition and consumer choice.

As a result of this industry pushback, the Commission sent a letter to the EBA in May 2017, indicating that it intended to amend the RTS to introduce a requirement for ASPSPs to have contingency measures in place allowing TPPs to access payment accounts through a user-facing interface in case of unavailability or inadequate performance of a dedicated TPP interface.

However, the banking industry has voiced concerns that this fallback carries with it the same security and data risks posed by screen scraping, as well as increased costs for ASPSPs who will need to build, maintain and test two

interfaces.

The EBA published an Opinion on 29 June 2017 responding to the Commission's proposed amendments. The EBA explained that whilst it agreed with the Commission's principles, it disagreed with the proposed amendments as it considered they would negatively impact the fine trade-offs and balances between competing aims that it had sought to achieve when drafting the RTS.

The Commission must now make a final decision on the text of the RTS and formally adopt the standards. It remains to be seen whether the Commission will retain its proposed amendments, including the "screen scraping" access fallback provision. Once adopted by the Commission, the RTS will be subject to scrutiny by the EU Council and Parliament before being published in the Official Journal.

TPP access during the transitional period and SecuRe Pay Guidelines

The RTS will not start to apply until 18 months after publication in the Official Journal, which means there will be a period of well over a year where the Level 1 requirements relating to TPP access will apply, but the related RTS will not.

Both the EBA and Commission have expressed their views that existing TPPs must not be prevented from continuing to provide services during this transitional period. In its report accompanying the final draft RTS, the EBA confirmed that pre-existing AISPs, PISPs and CBPIIs "*shall not be forbidden to continue to perform the same activities during the transitional period*" meaning that ASPSPs would need to allow these TPPs access.

The Commission also addressed how these requirements fit with existing EBA guidelines on security of internet payments, which are based on the recommendations of the European Forum on the Security of Retail Payments (SecuRe Pay). It states in its FAQ on PSD2 that "*[w]hen the EBA Guidelines are applied by the competent authorities of the Member States, in the transitional period, they must be interpreted in so far as there is any scope to do so, in line with the PSD2's content and objectives. As a consequence, compliance with the EBA Guidelines on the security of internet payments should not be used to justify obstructing or blocking the use of PIS or AIS*".

Effectively, this means that ASPSPs may need to permit TPPs access to payment account via screen scraping during the transitional period, unless and until an alternative solution is developed.

In the UK, HM Treasury and the FCA have confirmed that they expect firms to "*adhere to the principles of safety and security from day one*" but that ASPSPs must not block access via "screen scraping", unless they provide another access route which TPPs can use without having to comply with requirements yet to come into force. This suggests that banks will not be able to require TPPs to follow a full authentication process that requires compliance with the requirements of the RTS, although is it not entirely clear.

API and open banking – a possible solution?

At the same time, HM Treasury and the FCA are encouraging the industry to develop APIs as the basis for TPP access to payment accounts, and to transition to use of secure APIs "*as soon as possible during 2018*".

The Competition and Markets Authority (CMA) is already requiring nine UK banks to adopt open API standards as part of its "Open Banking" project.

Whilst the scope of the Open Banking project is narrower than PSD2 and so will not apply to all ASPSPs and payment accounts to which TPPs may require access, HM Treasury and the FCA are encouraging ASPSPs to adopt Open Banking APIs more broadly.

Under the Open Banking project, secure APIs are being developed according to common standards and using secure common infrastructure where necessary. Therefore, TPPs should not need to integrate with different technology on a firm-by-firm basis, where ASPSPs allow TPPs access via secure APIs based on Open Banking standards. It remains to be seen how broadly this standard will be adopted but use of secure open APIs currently seems to be the most promising solution for TPP access.

Liability allocation

PSD2 introduces a liability waterfall such that the ASPSP is, by default, liable to the customer for non-execution, defective or late execution of payment transactions involving a TPP, regardless of whether it or a TPP is at fault.

Under Article 73 PSD2, the payer's ASPSP must refund the payer the amount of any unauthorised payment transaction immediately (and in any event no later than by the end of the following business day) after noting or being notified of the transaction, except where it has reasonable grounds for suspecting fraud and communicates those grounds to its national regulator in writing.

Similarly, under Article 90 PSD2, the payer's ASPSP must refund the payer the amount of a non-executed or defective payment transaction initiated through a TPP and, where applicable, restore the debited payment account to the state it would have been in had the defective transaction not taken place. However, in contrast to Article 73 PSD2, Article 90 does not specify how quickly the ASPSP must make the refund or restore the account.

Whilst the ASPSP remains liable towards the PSU, if a TPP is at fault for the unauthorised payment transaction under Article 73 or for the non-execution, defective or late transaction under Article 90, the ASPSP is entitled to claim immediate reimbursement from the TPP. In each case, the burden lies with the TPP to prove that "*within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to"* the transaction in question. In this context, "immediate" reimbursement means no later than the end of the next business day.

Nevertheless, this means that the ASPSP potentially takes credit risk on an unknown TPP and so there remains a risk of loss if the TPP is unable to pay. As noted above, PIS providers are subject to relatively low capital requirements and whilst they are required to have PII or a comparable guarantee covering their activities, there are concerns that suitable PII may not be available.

These requirements are "without prejudice" to Article 71 PSD2, which places a 13 month time limit on the ability of a PSU to seek rectification of an unauthorised or incorrect payment transaction (provided that the PSP complied with relevant information requirements). However, where the PSU is not a consumer (or micro-enterprise), PSPs can agree a different time limit under the corporate opt-out.

ASPSPs will need to consider, and may wish to document, how their processes for refunding customers and seeking reimbursement from a TPP

will work in practice. In this regard, ASPSPs should consider what information or other assistance they may require from customers in pursuing a claim against a TPP and whether they may seek to include provisions addressing these issues in customer documentation.

CBPIIs

PSD2 also seeks to facilitate new issuers of payment instruments (particularly debit cards), which can be linked to an account held by the card user with an unrelated ASPSP.

In particular, PSD2 requires that, upon receipt of a request from a CBPII to confirm whether there are sufficient funds in the payment account for the relevant payment to be made, the ASPSP must provide a yes or no answer on the availability of the amount of funds requested "immediately", provided that the request complies with certain requirements, including that:

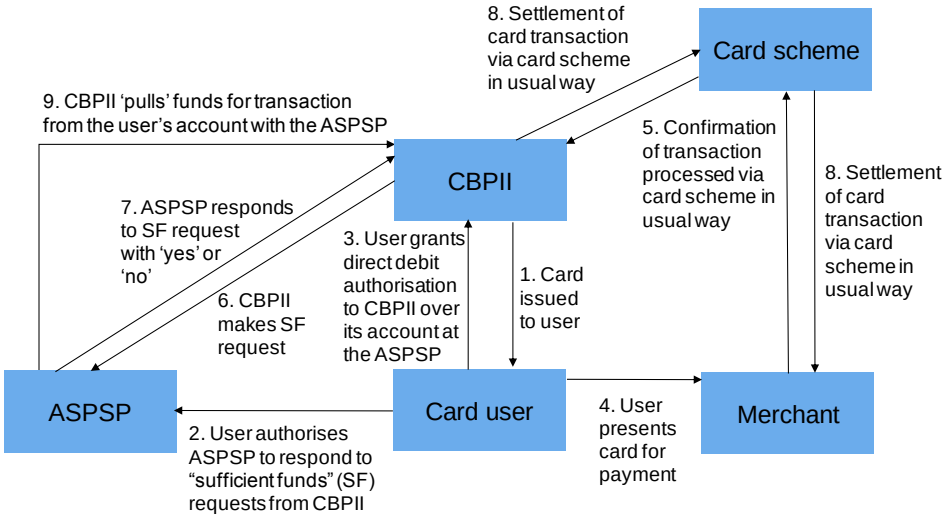
- the customer has provided its explicit consent to both the CBPII and the ASPSP (see "*Consent and data protection*" below for further discussion about this requirement); and
- the account is accessible online. In its draft approach document, the FCA clarifies that in a CBPII context, the account must be "*accessible online for the purpose of giving the yes/no answer. The account does not need to be accessible to the customer to check their balance*."

The FCA has also indicated in its draft approach document that the requirement for the ASPSP to respond "immediately" to a request from a CBPII means that the response should be "*sufficiently fast so as not to cause any material delay in the payment transaction*".

Therefore, banks and other ASPSPs may need to review their systems and processes to ensure they are able to respond to requests from CBPIIs within a very short timescale, even for accounts in respect of which the ASPSP does not itself offer cards. It is clear that for some ASPSPs, this will mean a material upgrade to existing functionality.

PSD2 does not govern subsequent settlement of the transaction between the payee, CBPII and the payer, which may vary between different business models. Therefore, CBPIIs may agree with their customers whichever settlement model they choose, although the way in which the service is structured may impact the types of payment services a CBPII is providing and therefore which permissions it may need. The diagram below illustrates a potential model that some CBPIIs may adopt.

A potential CBPII model



CONSENTS

Consent for payment transactions

Article 64 PSD2 (which was Article 54 PSD1) provides that a payment transaction is considered to be authorised if the payer has given consent to the relevant transaction or series of transactions in the form agreed with its PSP. For example, consent could be given in writing, verified by a signature, by means of a payment card and PIN number, over a secure password-protected website, by telephone or by use of a password. Consent may also be given via the payee (e.g. in the case of a direct debit) or, now, via a PIS provider.

A PSU may withdraw consent for a payment transaction or series of transactions at any time up to the point that the transaction is deemed irrevocable under Article 80 PSD2. However, this is subject to the corporate opt-out, meaning that PSPs can agree earlier cut-off times for withdrawing consent with corporate clients.

Consent in relation to personal data and overlap with GDPR

Article 94(2) of PSD2 provides: "*Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user*." Whilst unclear, this provision seems to refer to personal data relating to the PSU itself, and therefore to circumstances where the PSU is an individual rather than a legal person.

Therefore, PSPs will be required to obtain explicit consent from an individual PSU to cover processing of his or her own personal data for the provision of the relevant payment services. However, this requirement seems unnecessary, as these individuals are already protected by the requirements of the Data Protection Act in the UK, and will in the future be protected by the GDPR, in relation to the processing of their personal data. This can lead to some unhelpful consequences given the potential for divergent approaches under Article 94(2) PSD2 and GDPR.

Consents

- PSUs must give consent for payment transactions
- Consent for a transaction or series of transactions may be withdrawn before the moment of irrevocability (subject to corporate opt-out)
- Individual PSUs must give explicit consent for access, processing and retention of personal data
- PSUs must give explicit consent to TPPs for them to access payment accounts
- Card users must give explicit consent to CBPIIs and ASPSPs before a CBPII can request confirmation of availability of funds

Neither PSD2 nor the PSRs 2017 defines what is meant by "explicit consent" in this context. However, the FCA states in its guidance on the PSRs 2017 that PSPs should take account of the Information Commissioner's (IC's) guidance on the meaning of "explicit consent", albeit whilst cryptically "*keeping the objectives and specific context of the PSRs 2017 in mind*".

Firms will need to consider how to implement these requirements in respect of both new and existing customers and in light of their GDPR strategy.

TPP access and consent

TPPs that provide PIS and/or AIS are permitted to seek access to a payment account only with the PSU's explicit consent (under Articles 66 and 67 PSD2, respectively). In its draft approach document, the FCA notes that it is the TPP's responsibility to ensure the PSU has provided consent and that TPPs should make available to customers the information they need to "*make an informed decision and understand what they are consenting to (e.g. they must be able to understand the nature of the service being provided to them and the way that their information will be used)*".

The FCA has also confirmed that by contrast, ASPSPs are not required to obtain consent or check the terms of the consent provided by the customer to a TPP providing PIS and/or AIS.

CBPIIs and consent

Under Article 65 PSD2, where a card user wishes to use a CBPII, it must:

- provide explicit consent to the ASPSP to respond to requests from a CBPII to confirm that there are sufficient funds in the account for the transaction; and
- provide explicit consent to the CBPII to request this confirmation.

The card user must have provided its consent to the ASPSP before the CBPII makes its first request for a confirmation. This therefore seems to be a one-off consent, given to the ASPSP in respect of a particular CBPII.

The FCA has expressed its view that it would "*not be sufficient to include wording in a framework contract to the effect that the customer consents to the ASPSP confirming availability of funds whenever requests come in, nor would any form of "deemed" acceptance be acceptable*". A CBPII will therefore need to ensure that the customer has provided this consent to its ASPSP before it starts making requests.

On the other hand, the consent to the CBPII must be given on a transaction by transaction basis. In its draft approach document, the FCA states that the CBPII "*should be clear in its framework contract with the customer how consent is provided in relation to individual requests for confirmation of availability of funds (e.g. through the customer entering personalised security credentials at the point of sale)*".

Summary of consents required under PSD2

PSD2 Article	Required consents	PSD1
Article 64	PSU → PISP or ASPSP	✓ (except via PISP)
Article 65	PSU → CBPII PSU → ASPSP	× (new for PSD2)
Article 66	PSU → PISP	× (new for PSD2)
Article 64	PSU → AISP	× (new for PSD2)
Article 94(2)	PSU → PSP	× (new for PSD2)

SECURITY

PSD2, like GDPR and the Network and Information Security Directive (NIS Directive), introduces various new requirements aimed at enhancing security. PSD2 includes requirements for PSPs to:

- submit to their national regulator an annual assessment of the operational and security risks relating to the payment services they provide and of the adequacy of the mitigation measures and control mechanisms implemented in response to those risks;
- maintain effective incident management procedures to detect and classify major operational or security incidents relating to payment services and notify their national regulator of any such incidents;
- notify its customers directly, and without undue delay, if a security incident might impact the financial interests of those customers; and
- apply "strong customer authentication" (SCA) when a PSU accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel that may imply a risk of payment fraud or other abuse.

Firms will need to update their current policies and procedures to reflect these requirements and assess the potential impact of these security-related requirements on their business operations more generally.

PSPs applying for authorisation as payment institutions under PSD2 will also need to submit a copy of their security policy, including a detailed risk assessment and a description of security control and mitigation measures taken to protect PSUs against risks identified, including fraud and illegal use of sensitive and personal data.

Security

- New transaction authentication requirements and rules on secure communications
- New incident management and reporting regime for major operational and security incidents
- Requirements for PSPs to have a security policy, security control and mitigation measures and security incident management procedures

Strong customer authentication or SCA

PSD2 places great emphasis on the security of internet payments and introduces the concept of SCA, which is authentication based on the use of two or more elements categorised as:

- knowledge (something only the user knows);
- possession (something only the user possesses); and
- inherence (something the user is).

These elements must be independent, so that the breach of one does not compromise the reliability of the others and must be designed in such a way as to protect the confidentiality of the PSU's personalised security credentials. Authentication of remote electronic payment transactions must include elements which dynamically link the transaction to a specific amount and specific payee.

As noted above, the EBA has drafted RTS on SCA and CSC, which are currently awaiting adoption by the Commission. These RTS specify technical requirements for SCA, set out exemptions from their application and the requirements with which security measures have to comply in order to protect the confidentiality and integrity of PSUs' personalised security credentials.

In general, PSPs must apply SCA where a PSU accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse (for example, setting up a new payee). However, the RTS provide for exemptions from the application of SCA, including for:

- low value contactless payments,
- recurring payments to the same payees which have been previously set up using SCA
- payments at ‘unattended terminals’ for transport or parking fares; and
- transactions identified as low risk as a result of 'transaction-risk analysis'.

The EBA has acknowledged the trade-offs that it has needed to make when drafting the RTS, including, how prescriptive (or high level) the requirements should be and therefore what level of flexibility should be afforded to PSPs now and in the future. The EBA explained it also sought to balance customer convenience with the greater level of security that may be achieved by subjecting the customer to multiple security and authentication steps.

PSD2 also links use of SCA to the allocation of liability. It provides that if the payer's PSP does not require SCA, the payer will be liable for a disputed transaction only where it has acted fraudulently, and if the payee or its PSP does not accept SCA, then that party shall refund the payer's PSP for any unauthorised payment.

Whilst the RTS on SCA will not apply until 18 months after their publication in the Official Journal, the high level requirements on SCA in PSD2 will apply from 13 January 2018, including (oddly) the provisions on allocation of liability in the event SCA is not applied. Therefore, firms should consider how they intend to comply with these requirements and how they might impact their systems, processes and documentation.

Incident management and reporting

PSD2 requires PSPs to maintain effective incident management procedures to detect and classify major operational or security incidents relating to payment services. PSD2 also requires PSPs to notify their national regulator "without undue delay" of any major operational or security incident.

The EBA has published final guidelines setting out the criteria, thresholds and methodology to be used by PSPs to determine whether or not an operational or security incident should be considered major (and therefore subject to the notification obligation). These include the total value and number of transactions and PSUs affected, service downtime, economic and reputational

impacts, level of internal escalation and whether it may have a systemic impact on other payment services or infrastructures.

The guidelines also include templates that PSPs should use for these notifications and ongoing reporting during the lifecycle of a major incident and specify the timeframes for making notifications and reports. In response to industry feedback, the EBA has extended the deadline for making the first report from 2 hours to 4 hours from the moment the incident was first detected. It has also clarified that 'near misses' do not need to be reported.

The guidelines allow PSPs to delegate their incident reporting obligations to a third party, provided that certain conditions are met. In some circumstances, they also allow PSPs to report incidents through a service provider in a consolidated manner with other affected PSPs.

In its report accompanying the final guidelines, the EBA acknowledged that other incident notification frameworks exist and explained that it has therefore sought to align the PSD2 incident reporting guidelines as far as possible with the cyber incident-reporting framework for banks under the Single Supervisory Mechanism. However, the EBA stated that alignment with other similar incident reporting frameworks (such as under the GDPR and the NIS Directive, which will both apply from May 2018) went beyond its mandate.

Therefore, many firms will have to contend with implementing this triple cocktail of similar (but not identical) incident reporting requirements under PSD2, GDPR and the NIS Directive over the coming months. In any case, firms will need to review their existing incident management and reporting systems and processes, in order to assess what changes they may need to make in order to comply with these PSD2 requirements and guidelines.

COMPLAINTS HANDLING AND DISPUTE RESOLUTION

PSD2 introduces changes to complaints handling and dispute resolution rules, including a requirement for PSPs to respond to payment services complaints addressing "all points raised" within 15 business days (and 35 business days in exceptional circumstances, in which case a holding reply must be provided first).

These requirements introduce a minimum standard for complaints handling across the EU, although Member States are able to introduce or maintain dispute resolution rules that are even more favourable to the PSP. See "*Member State options for implementation*" below for other examples of Member States' discretions and options when implementing PSD2.

Under Article 102 PSD2, PSPs must also have effective procedures to handle complaints before a dispute is referred to alternative dispute resolution (ADR) or brought before a court. In the UK, eligible complainants will be able to refer payment services disputes to the Financial Ombudsman Service (FOS). Eligible complainants will generally include consumers, microenterprises and small charities (i.e. PSUs for which a PSP cannot exercise the corporate opt-out).

In relation to non-eligible complainants, HM Treasury has confirmed that under Regulation 101 of the PSRs 2017, PSPs need to notify a complainant about sources of ADR only where that PSP actually uses ADR services. It therefore appears that the UK has exercised its option to disapply Article 102 where the PSU is a corporate.

The FCA will also require firms to submit a periodic "payment services complaints" return, setting out the total number of payment services and e-money complaints they received, broken down by the number of complaints for each type of service provided. These requirements apply to all complaints from payment service users, whether or not they are eligible complainants for the purposes of referring complaints to the FOS.

Implementation and next steps

Member State implementation

The fact that PSD2 is a Directive, which needs to be transposed into national law in each Member State, has a number of consequences for firms seeking to implement its requirements.

Firstly, there is a risk that not all Member States will transpose PSD2 into national law by the deadline of 13 January 2018. For example (and as noted above) Sweden has recently confirmed that it does not intend to implement PSD2 until May 2018. Therefore, in some jurisdictions, existing rules under PSD1 may continue to apply past 13 January 2018.

Even for jurisdictions that do meet the transposition deadline, firms may have only a short period between publication of the final legislation and rules implementing PSD2 and application of the relevant requirements. As at September 2017, only around half of Member Stated had published implementing measures. In the UK, whilst the final PSRs 2017 have been published, the FCA has not yet published final Handbook changes or its final approach document. In the absence of final implementing legislation and rules in many Member States, firms may need to base their implementation plans on the text of PSD2 itself, or on draft implementing legislation and rules, if available.

This timing issue is compounded by the fact that PSD2 allows Member States to exercise various options and discretions when implementing its requirements (see "*Member State options for implementation*" below for further detail). Some Member States may also decide to "gold plate" PSD2 requirements, by applying PSD2 standards more widely and/or imposing requirements that go beyond those set out in PSD2.

Member State options for implementation

PSD2 grants Member States various discretions and options when implementing its requirements. Whilst some of these are carried across from PSD1, others are new. Several of these options also relate to provisions already subject to the corporate opt-out. Therefore, PSPs should check carefully the approach being taken by relevant Member States in respect of these options in order to assess their impact.

These options and discretions include the following:

- ***Small payment institutions***: Member States may exempt small payment institutions from authorisation and the application of most prudential requirements
- ***No corporate opt-out for microenterprises***: Member States may apply the provisions of Titles III and IV PSD2 to microenterprises in the same way as to consumers.
- ***Monthly statements in a durable medium***: Member States may require PSPs to provide at least monthly statements, on paper or using another

durable medium, free of charge.

- ***Changes to derogation threshold amounts***: For national payment transactions, Member States or regulators may reduce or double the threshold amounts for low-value and e-money payments (of €30 per transaction or €150 spending or storage limit) for the derogation from information requirements and certain Title IV requirements. They may also increase the threshold amounts for prepaid instruments up to €500 and limit the derogation under Article 63(3) to e-money accounts or instruments of a certain value.
- ***Prohibition or limitation on surcharging***: Member States may prohibit or limit the right of the payee to request a surcharge on certain payment instruments
- ***More favourable termination rights***: Member States may provide for more favourable provisions for PSUs to terminate a framework contract than those set out under Article 55 PSD2
- ***Payer's liability for unauthorised transactions***: Member States may reduce the payer's liability for unauthorised transactions (from a limit of €50) taking into account relevant circumstances.
- ***Refund rights for non-euro direct debits***: Member States may require PSPs to offer refund rights for non-euro direct debits that are more advantageous to the payer than those set out in Article 76 PSD2.
- ***Shorter execution times***: For national payment transactions, Member States may provide for shorter maximum execution times than those provided for in Section 2 of Title IV PSD2.
- ***More frequent risk assessments***: Member States may require PSPs to provide risk assessments more frequently than annually (which is the minimum frequency required).
- ***More favourable dispute resolution rules***: Member States may have dispute resolution rules that are more favourable to PSUs that those outlined in Article 101(2) PSD2.
- ***ADR limited to consumers***: Member States may provide that the requirements relating to availability of ADR at Article 102 PSD2 do not apply where the PSU is a corporate.
- ***Transitional authorisation for existing payment institutions***: Member States may grant automatic authorisation to existing payment institutions for a transitional period until 13 July 2018, provided that certain conditions are met.

Customer account documentation changes

Key changes to customer account documentation may include:

- Corporate opt-out for agreements brought within extended scope of PSD2
- Provisions relating to TPP access and circumstances in which the ASPSP may refuse access
- Requirement for customer to provide assistance (e.g. information) where the ASPSP seeks reimbursement from a TPP
- Terms relating to application of SCA
- Terms relating to the customer's obligations in case of a security breach or other incident
- Updating of complaints and dispute resolution provisions

UK approach to implementation and optionality

HM Treasury explained that when implementing PSD2 through the PSRs 2017, it has generally taken a copy-out approach, whilst looking to take advantage of derogations and ensuring that the exemptions from PSD1 carry across to PSD2, where appropriate.

For example, under the PSRs 2017, small PSPs can benefit from a registration regime with fewer prudential requirements, PSPs cannot apply the corporate opt-out to microenterprises or small charities, and in relation to derogations for low-value and e-money payments, the threshold amounts have been set at the maximums permitted.

In relation to provision of statements in a durable medium, HM Treasury has explained in its feedback to its consultation on the PSRs 2017, that the UK

government's intention is to mandate that customers are provided with a monthly statement on a durable medium, but that it "*intends to also allow PSPs to include in their framework contracts a clause which enables consumers to choose...whether they wish to have the statement actively provided or just made available on request, whether they wish to receive it in an alternative manner which allows the information to be stored and reproduced, and whether they wish to receive it more frequently than monthly*".

Therefore, PSPs are permitted but not required to include terms in a framework contract allowing customers to receive statements more than monthly and in media more in keeping with the PSP's business.

Next steps

If they have not done so already, firms should promptly identify the practical steps they will need to take in order to implement PSD2. The first step will be to identify changes that are absolutely necessary for 13 January 2018 and those that are not.

Key implementation areas are likely to include:

- technology and systems build, for example development of an open API for TPP access;
- client documentation changes, for example take into account the increased scope of PSD2 and reflect changes to security requirements;
- client communications, including notifications about a refusal to allow a TPP access or a security incident that might impact the client's financial interests;
- policies and procedures, including a security policy, procedures for incident reporting and dispute resolution procedures; and
- reauthorisation requirements for authorised payment institutions, with more information required as part of the application.

Firms will also need to consider how each relevant Member State intends to implement PSD2, to ensure their implementation plans take into account the way in which these Member States are exercising any options and discretions, as well as any gold plating. Since this may not be known until a relatively late stage, firms may need to keep this under review and build a level of flexibility into their implementation plans to allow them to adapt to the way in which different Member States decide to implement PSD2.

Following implementation, firms may also wish to carry out a benchmarking exercise, to ensure that their approach to implementation, for example in relation to client documentation, is not out of step with the market.

CONTACTS

Caroline Meinertz
Partner

T +44 20 7006 4253
E Caroline.Meinertz
@cliffordchance.com

Peter Chapman
Senior Associate

T +44 20 7006 1896
E Peter.Chapman
@cliffordchance.com

Simon Crown
Partner

T +44 20 7006 2944
E Simon.Crown
@cliffordchance.com

Maria Troullinou
Senior Associate

T +44 20 7006 2373
E Maria.Troullinou
@cliffordchance.com

Mardi MacGregor
Lawyer

T +44 20 7006 3354
E Mardi.MacGregor
@cliffordchance.com

Kikun Alo
Senior Associate

T +44 207006 4067
E Kikun.Alo
@cliffordchance.com

Meera Ragha
Lawyer

T +44 20 7006 5421
E Meera.Ragha
@cliffordchance.com

Laura Douglas
Professional Support Lawyer

T +44 20 7006 1113
E Laura.Douglas
@cliffordchance.com