CLIFFORD
CHANCE

Clifford Chance Client Briefing

June 2015

Payment Services Directive 2

On 2 June 2015, the Council of the EU published its final compromise text for the new Payment Services Directive (the Directive). Further substantive amendment is not expected before the legislation's imminent adoption.[1] Existing payment service providers (PSPs) – including banks – will have to change systems and processes to comply with the new rules, which are expected to apply from mid-2017. The Directive also raises a number of strategic questions on how to balance access with security.

The fast pace of change in mobile, online and electronic payments has shaped this latest overhaul of the EU framework for the regulation of payment services. The Directive will repeal the 2007 Payment Services Directive (PSD1) and will broaden the scope (and increase the burden) of payment services regulation in the EU. The Directive is set to increase security and transparency requirements while bringing some "one leg out" transactions and transactions in non-EU currencies into scope for the first time.

The Directive retains the same basic structure as PSD1 and is organised into six titles with Title I covering scope and definitions, Title II dealing with the authorisation and regulation of payment service providers (PSPs) and Title III addressing transparency. Title IV establishes the respective rights and obligations of payment service users (PSUs) and PSPs while Titles V and VI set out provisions on delegated acts and the implementation timetable. The Annex to PSD1 listing the different categories of payment service remains and is largely unchanged apart from the addition of payment initiation and account information services.

Scope

Territorial scope

Many provisions of Title III and Title IV of the Directive will now apply to a broader range of payment transactions. Specifically, transactions in non-EU currencies where both the payer's and the payee's PSP (or the sole PSP in the transaction) are located in the EU will be caught, as will payment transactions in all currencies where only one PSP is located in the EU ("one leg out" transactions). Such payment transactions were outside the scope of PSD1, but are now brought in scope "in respect of those parts of the payment transaction which are carried out in the Union" – not the clearest geographic delineation!

Negative scope exemptions

The Directive makes changes to some of the negative scope exemptions established in PSD1. Changes to the "commercial agent" exemption now make clear that this exemption applies when agents act only on behalf of the payer or payee (not both). Where agents act on behalf of both parties (such as in the case of some e-commerce platforms), there is scope to rely on the exemption but only in cases where the

Jargon buster

Account servicing payment service provider (ASPSP) – these are typically traditional financial institutions and in the Directive the term generally refers to the bank of the payer or payee in the context of payment transactions made via online banking.

Payment initiation service provider (PISP) – this definition envisages newer entrants to the payments market who provide a software "bridge" between a payer and the PSP of that payer (normally a bank) to facilitate online payments by initiating an order at the request of the payer. Often the PISP has no contract with the ASPSP of the payer.

Account information service providers (AISP) – this type of PSP provides PSUs with aggregated online information for multiple payment accounts held with multiple ASPSPs and accessed via the online systems of those ASPSPs. This service provides the PSU with an instant and overall view of their financial situation on several accounts with different providers.

Third party payment service provider (TPP) – means either a PISP or an AISP.

Payment service user (PSU) – means that underlying user of services provided by PSPs.

[1] Unless otherwise specified, references to the Directive in this briefing are to the final Council compromise text of 2 June.

agent does not come into possession or have control of clients' funds. This addresses member states' divergent implementation of PSD1.

Use of the "limited network" exemption is also being restricted. Under the new rules, it will not be possible to use the same payment instrument within more than one limited network or to acquire an unlimited range of goods and services. The changes are designed to limit use of the exemption to genuinely small networks – shopping mall and employer dining cards, for example.

The Directive places quantitative caps that will limit the use of the mobile device content exemption. This exemption facilitates "operator billing" or direct to phone-bill purchases such as ring tones, premium SMS-services, music and other digital content downloads, as well as voice-based services. The new rules will limit use of the exemption to individual payments that do not exceed EUR 50 and on a monthly basis to transactions not exceeding EUR 300 in aggregate per subscriber.

In its original proposal for the Directive, the Commission indicated that the current ATM exemption (in Article 3(o) of PSD1) should be deleted completely. However, in the final text, the ATM exemption has survived but ATM operators will be subject to obligations to provide customers with information on withdrawal charges both prior to the transaction and on the customer's receipt, aiming to enhance transparency.

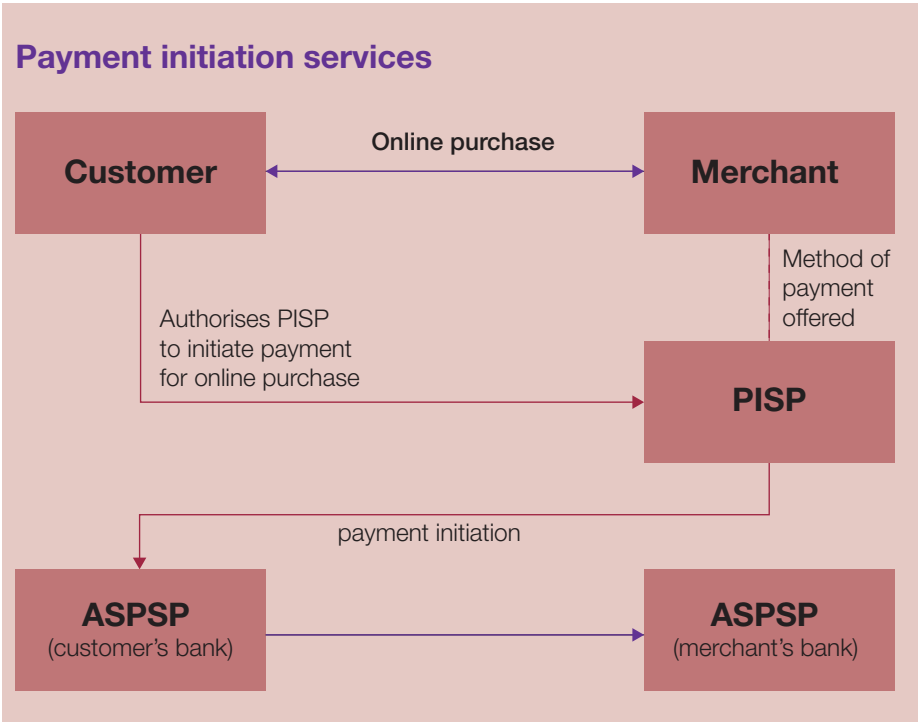
The Directive also contains provisions seeking to minimise divergent interpretations and application of certain exemptions (notably the limited network and the mobile content exemptions discussed above), which arose as a result of the self-assessment approach of PSD1. Accordingly, PSPs under the Directive have to notify relevant activities to competent authorities, so that an assessment can be made as to whether the requirements in question have been met.

Third party payment services

Payment initiation services

Third party payment service providers (TPPs) are a focus of the Directive and their inclusion was possibly the most controversial aspect of the legislative negotiations. Payment initiation service providers (PISPs) are probably the most important category of TPP and payment initiation services are at the heart of online banking transactions. Typically, to effect online banking transactions, the payer is not just sharing its personal security credentials with its bank but also has to transmit that data via one or more third party software providers who provide the interface through which the customer accesses its online account and transmits the payment.

Essentially, the PISP is a facilitator that enables the transmission of funds, by populating the transaction details and confirming that the payer has sufficient funds in its account to execute the transaction in question (see diagram below). The PISP will not receive or handle customer funds at any stage and will not provide a statement of account balance; it will merely give a 'yes' or 'no' answer as to whether the payer has sufficient funds in his/her account to complete the transaction in question. As a precondition to offering this service, the payer has to have given its explicit consent to the account servicing payment service provider (ASPSP) to respond to requests from a specific PISP prior to the first request for confirmation being made. The Directive also imposes obligations on PISPs



when offering this service, including the requirement to authenticate themselves and to communicate securely with the ASPSP for each confirmation request.

The Directive prevents ASPSPs from requiring PISPs to have a contract with them as a pre-condition of provision of the initiation service. In other words, banks cannot force PISPs to agree terms governing their responsibilities and liabilities when accessing the PSU accounts. Although designed to stop anti-competitive behaviour, the rule runs contrary to the broader cyber security agenda set in the Directive and elsewhere.

Under the Directive, PISPs are required to be authorised but are subject to a reduced minimum own funds requirement (of EUR 50,000). PISPs also have to hold professional indemnity insurance or a comparable guarantee in order to ensure that they are able to meet liabilities arising in relation to their activities. Where a PSU's payment account is online, the Directive guarantees the PSU a right to use the services of a PISP. The Directive compels banks and other ASPSPs to take specific steps to ensure that payments made via a PISP (and which the PSU has authorised) are handled by the ASPSP promptly and in a non-discriminatory way.

The treatment of PISPs in the Directive is a response to their emergence since 2007 and recognises their potential to play an increasingly important role in the market. The Directive aims to subject PISPs to a level of supervision commensurate with the risk they introduce into the system whilst preventing traditional PSPs like banks from stifling the role of PISPs – whether the balance struck will work, remains to be seen.

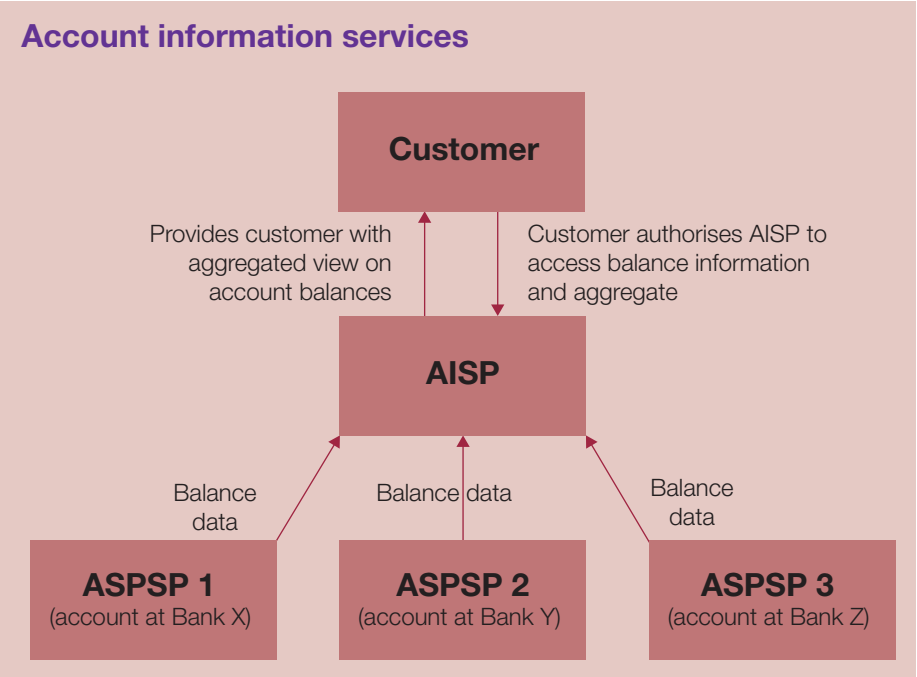
Account information services

The key function of account information service providers (AISPs) is to aggregate information from payment accounts maintained by other institutions – usually banks. To do this, AISPs need access to those payment accounts. For online payment accounts, the Directive requires banks and other ASPSPs to respond to data requests from AISPs in a non-discriminatory manner. The Directive's provisions on AISPs are similar to those established for PISPs. To some extent they recognise the role that AISPs already play in the market and are designed to allow AISPs to compete and collaborate with more traditional players. Under the Directive, PSUs will have a right to use AISPs in online transactions and banks and other payment institutions will effectively be prevented from thwarting the business of AISPs, tying AISPs into contracts with them or forcing AISPs to adopt particular business models and practices.

AISPs are expressly exempt from authorization under the Directive, but they will have to register. Even though they are not subject to regulatory capital requirements, AISPs will (like PISPs) be obliged to hold professional indemnity insurance or a comparable guarantee in order to ensure that they are able to meet liabilities arising in relation to their activities.

Bank accounts for PSPs (including TPPs and other non-bank payment institutions)

The Directive adds a new provision that requires member states to ensure that all payment institutions have access to payment account services provided by banks. This includes not only the new category of third party intermediaries like PISPs and AISPs but also other payment institutions like money remitters. This provision is designed to prevent banks from refusing to open and maintain bank accounts for non-bank



payment institutions. Although the ability of a bank to reject account applications on valid grounds (such as anti-money laundering concerns) would not be affected, banks that decline to provide a bank account to another payment institution will have to explain the rejection to the regulator.

Security and liability

Security

The Directive introduces and defines the concept of "strong customer authentication" and requires PSPs to apply strong customer authentication where a PSU accesses their online account or initiates a payment transaction. These provisions are intended to strengthen the security of internet based payments and promote consumer protection. The final detail relating to strong customer authentication will be specified by the EBA, in close cooperation with the ECB, via Level 2 technical standards and guidance.

Liability for unauthorised transactions

PSPs are liable for unauthorised payment transactions although PSUs may be obliged to bear losses up to EUR 50 (reduced from EUR 150 under PSD1) in cases of lost or stolen payment instruments.

The Directive also amends the liability provisions of PSD1 to take into account the introduction of the new TPP players into the payment services arena. Under the Directive, each PSP takes responsibility for the respective parts of the transaction under its control. Accordingly, where a PSU initiates a payment transaction through a PISP, the burden of proving proper authentication and accurate recording falls to the PISP. However, in the absence of a contract between a PISP and an ASPSP, the Directive (reflecting consumer protection concerns) still allows a payer to claim a refund from the ASPSP (even where a PISP has been involved).

While it remains to be seen how the allocation of liability provisions will operate in practice, the final text of the Directive does deal with some of the concerns that industry had raised in response to the Commission's original proposal. The final text provides that if the PISP is liable for an unauthorised, non-executed or defectively executed transaction or a payment transaction that was executed late, it shall immediately compensate the ASPSP at its request for sums paid or losses incurred as a result of any refund. However, concerns at the possibility of widespread losses caused by a thinly-capitalised PISP remain unaddressed.

Consumer protection

The Directive places a strong emphasis on transparency and consumer protection, seeking to build on the foundation laid under PSD1. In this respect, the Directive establishes a number of new provisions on fees and charges and introduces a new obligation imposed on the Commission to produce a leaflet for consumers setting out in a clear and comprehensible way their rights and obligations under the Directive.

Other legislation

There is an interplay between the Directive and other pieces of EU legislation. The Directive focuses

extensively on data protection and security issues and seeks to promote compliance with the relevant EU laws in this area (specifically the Data Protection Directives). References to the Network and Information Security Directive in the Commission's earlier draft proposal have now been replaced with an independent obligation under the Directive to maintain and establish incident management procedures, to report assessments on operational and security risks to competent authorities and to engage in incident reporting.

Implementing the Directive – things to think about...

- are previously out of scope accounts and/or transactions now in scope?
- how will our documentation need to change?
- are we or our clients relying on any of the exemptions that have been narrowed down?
- do we need to revisit our corporate opt-outs? What challenges or opportunities does this present?
- how do we spot a TPP? Could we be a TPP?
- which, if any, of our counterparties could be a TPP?
- how can we minimise our liability towards TPPs?
- are our systems in line with the security requirements?

Furthermore, the Directive introduces new provisions dealing with card surcharging which are intended to dovetail with both the new EU Regulation on Market Interchange Fees (the MIF Regulation) and also with the Consumer Rights Directive. In particular, payees will not be permitted to surcharge for card transactions where the interchange is regulated under the MIF Regulation (in other words, the quid pro quo for reducing merchant costs for card transactions is that the minimal cost that is charged will have to be internalised).

Next steps

The Directive will enter into force twenty days following its publication in the Official Journal. Member states will have until Q3 2017 to transpose the Directive into national law. As a full harmonization Directive, the risk of national "gold plating" should be limited but, based on the experience of PSD1, cannot be completely discounted.

Contacts

Simon Crown
Partner
T: +44 20 7006 2944
E: simon.crown@cliffordchance.com

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

Kikun Alo
Senior Associate
T: +44 20 7006 4067
E: kikun.alo@cliffordchance.com

Maria Troullinou
Senior Associate
T: +44 20 7006 2373
E: maria.troullinou@cliffordchance.com

Laura Douglas
Associate
T: +44 20 7006 3907
E: laura.douglas@cliffordchance.com

Dermot Turing
Consultant
T: +44 20 7006 1630
E: dermot.turing@cliffordchance.com

J20151206152054