A mid-summer storm: The key changes introduced by PSD2

As the payments industry was preparing for the summer holidays, the European Commission (the "**Commission**") released its much anticipated Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC ("**PSD2**"). As explained in our client briefing entitled "Updating the Payment Services Directive – PSD2", PSD2 builds on various European initiatives since the publication of the Commission's Green Paper on Card, Internet and Mobile Payments and aims to reflect new developments in the payments market.

PSP – payment service provider

PSU – payment service user

ASPSP – account servicing payment service provider

TPP – third party payment service provider

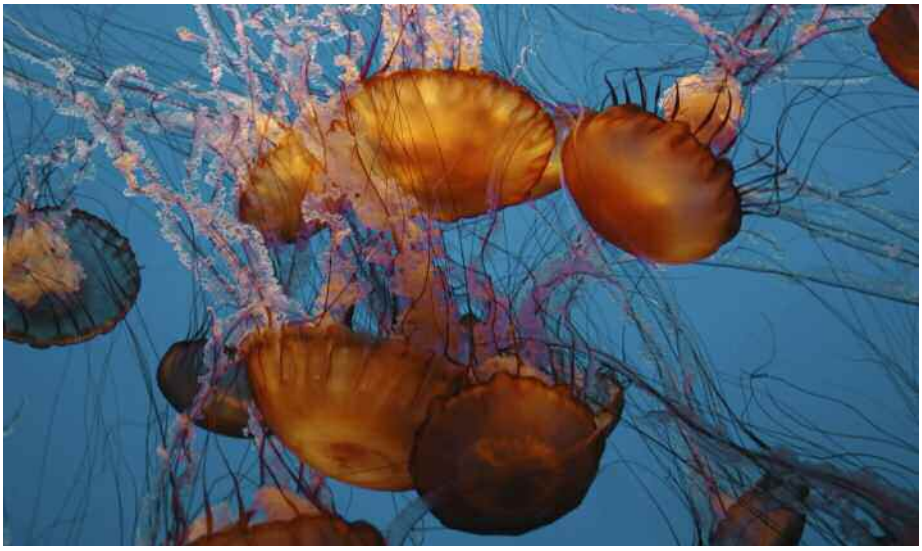
Expanding reach - from leg out to negative scope

Through PSD2 the Commission has sought to expand the regulatory reach of the existing Payment Services Directive ("**PSD**"), by using various tools, such as extending the so called 'leg-out' transactions to transactions with third countries where only one payment service provider ("**PSP**") is in an EU Member State, in respect of those parts of the payment transaction which are carried out in the EU. The impact of these provisions will vary between EU Member States, depending on their transposition of the relevant PSD2 provisions. It will be interesting to see how the determination as to which parts of a transaction are carried out in the EU will be made, in order to be in a position to take a view as to whether the PSD2 provisions apply. Moreover, the Commission has clarified that Title III will now extend to payments made in any currency and has amended the negative scope exemptions by clarifying - or rather narrowing - their scope. PSPs should consider whether their current arrangements have been affected by these changes and may have to revisit opt-out and operational clauses contained in customer documentation.

Protecting payment service users?

Having come closer to achieving a single market for payment services, the Commission is now looking at using payments legislation as a consumer protection tool. PSPs are no longer able to charge payers for making the appropriate notification in the event of loss/misappropriation of the relevant instrument and PSPs' relevant policies will have to be revisited and adapted accordingly.

An interesting development in this respect is the introduction of a new unconditional right of refund in respect of direct debits, except where the payee has already fulfilled its contractual obligations and the services/goods have already been received/consumed by the payer. PSPs are concerned as this refund right is conditional on facts that are outside of the inter-bank relationship, as well as the payee/creditor bank relationship, and could potentially result in them having to get involved in disagreements over whether payers have actually consumed or received the relevant goods or services, which may not be easily verifiable and provable. Moreover, the application of this concept to direct debit transactions is not feasible, as such payments operate on different premises to other types of payment. The amendments effectively turn a contractually agreed (optional) right into an absolute right and purport to bring the PSD2 regime in line with the SEPA Direct Debit Core Rulebook of the European Payments Council.



Here come the third party payment service providers

Arguably, the most significant amendment introduced by PSD2 has been the 'creation' of a new type of regulated entity, the third party payment service provider ("**TPP**"). This change is aimed at promoting innovation and low cost electronic payment solutions while ensuring that security and data protection are not compromised. TPPs offer services based on access to payment accounts provided by a PSP in the form of payment initiation services and/or account information services and will be subject to all PSD2 provisions applicable to payment institutions. The definition of a TPP carves out of its scope PSPs who provide and maintain payment accounts for a payer (i.e. account service providers, "**ASPSPs**"). PSD2 offers a (slightly confused) explanation as to what the account information service includes. EU Member States have to ensure that payers have the right to obtain payment card services by using a third party payment instrument issuer and ASPSPs are under an obligation to treat payment orders received in such a manner without discrimination, other than for objective reasons. It would be fair to say that the introduction of TPPs has brought a flood of changes to the payments landscape, including:

- making the authorisation application procedure more rigorous by requiring the submission of additional information including in respect of the procedure for security incidents and customer complaints, business continuity plans and policies on the collection of statistical data and fraud. Interestingly, smaller TPPs are effectively able to commence offering their services without prior authorisation.
- endorsing TPPs by obliging EU Member States to ensure that a payer has the right to use a TPP to obtain payment services enabling access to payment accounts. Under the PSD2 proposal, ASPSPs have to notify immediately the TPP of the receipt of a payment order and to provide information on the availability of funds on the payer's account (assuming that the payer has consented to such information being provided). PSD2 does not stipulate the terms of use of payment instruments where a TPP is engaged by a payment service user (a "**PSU**"), but does state that the PSP has to include within a framework contract a secure procedure to notify the PSU in the event of fraud. It has been suggested that PSPs are expected to find comfort in the fact that in the event of fraud or dispute the transaction reference and authorisation information should be made available to the ASPSP and the payer, when the TPP's own system was used to initiate the payment in question, but the relevant provision fails to clarify who decides whether a fraud or dispute has occurred or what constitutes a 'dispute'. This is tricky, especially as ASPSPs are not allowed to defer payment initiation where payment orders come via a TPP, nor to refuse payments initiated by a TPP for a payer. PSD2 also introduces the concept of deemed consent where the payer has authorised the TPP to initiate a payment transaction with an ASPSP, but the giving of consent in such form cannot be verified by the ASPSP which is under a legal obligation to protect the funds of the PSU.
- giving TPPs access to payment account information and empowering them to use such information. In return for such access, TPPs have to ensure that the personalised security features of the PSU are not accessible to other parties, to authenticate themselves in an "unequivocal" manner towards the ASPSP and to refrain from storing sensitive payment data or personalised security features of the PSU. It is the first time that PSUs are encouraged to communicate their personalised security features to a third party which is an interesting development in a world of proliferating online fraud, especially in light of the lack of clarity as to the elements of

the requisite level of authentication and the procedures for achieving it. But this is not the only provision of PSD2 that leaves questions unanswered. For example, what happens in a case where a notification by an ASPSP in respect of the receipt of a payment order and the availability of funds amounts to tipping off under anti-money laundering regulations? How (if at all) does PSD2 mitigate the risks that may arise by allowing third parties to gain access to information that is stored behind a PSP's secure firewall? It may be that the 'answer' to this question is that the relevant actors will have to adhere to regulatory security standards and the Cyber-Security Directive, but whether this would be an effective *ex ante* way of preventing misuse of the right to go behind another PSP's firewall remains to be seen.

- amending the liability allocation regime in an effort to reflect the new obligations and responsibilities and to cater for the introduction of new actors into the regulated payments services arena. It is questionable whether PSD2 adequately grapples with the task at hand, as despite the fact that the revised text seems to suggest that TPPs and ASPSPs can enter into contracts between them to allocate the liability in question, the actual legislative provisions are confused. Moreover, such documentation may not be well placed to address such issues. PSD2 effectively deems ASPSPs liable for unauthorised or incorrectly executed transactions even where a TPP is involved and, despite attempting to place the burden of proof on TPPs in certain cases, the reality is that the APPSP will have to compensate the PSU and attempt to resolve the liability issue later.

It remains to be seen whether the final PSD2 will manage to address the plethora of issues that the current proposal gives rise to. In a world of growing online fraud, it is crucial that the right balance is struck between innovation, security and consumer protection.

Contacts

Dermot Turing
Partner
T: +44 207006 1630
E: dermot.turing@cliffordchance.com

Simon Crown
Partner
T: +44 207006 2944
E: simon.crown@cliffordchance.com

Caroline Meinertz
Senior Associate
T: +44 20 7006 4253
E: caroline.meinertz@cliffordchance.com

Peter Chapman
Senior Associate
T: +44 207006 1896
E: peter.chapman@cliffordchance.com

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

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