LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Financial Regulatory Practice 26 April 2017 | Number 2122

Understanding PSD2: Key Points to Know About the Upcoming Regime[1]

New directive disrupts the EU payments regulatory regime. A series of Client Alerts will follow ongoing developments related to PSD2.

Key Points:

- By expanding the accessibility of customer account information, PSD2 allows third-party developers to build payment service infrastructures around the platforms of financial institutions.
- On February 23, 2017, EBA published the final draft Regulatory Technical Standards on strong customer authentication and common and secure communication, an important step toward the development of PSD2-compliant technological solutions.
- This first *Client Alert* provides a summary of the key aspects of the PSD2 to introduce the topic.

Latham will produce a series of *Client Alerts* to provide an overview of the key points of the upcoming regime introduced by the second Payment Services Directive (PSD2). [2] The upcoming regime was developed in light of the recent adoption of the final draft Regulatory Technical Standards on strong customer authentication and secure communication (RTS) by the European Banking Authority (EBA). [3]

This first *Client Alert* summarizes the key innovations and features of the PSD2 to introduce the topic and to clarify the development and implementation of this new regulatory regime.[4]

Overview

PSD2 allows third-party developers to build payment service infrastructures around the platforms of financial institutions. To achieve this result, banks will need to provide certain third parties with access to client account information, mainly via open APIs (Application Programming Interfaces). This new approach in the banking industry, also known as “open banking,” was introduced in the market in the wake of the disruptive appearance of non-bank players providing payment services in an industry typically dominated by financial institutions. Their success in challenging the market status quo from a competition law perspective was also a factor that boosted the adoption of PSD2.

Notably, while the idea of allowing payment initiation service providers to access customers’ payment accounts and requiring banks to make customer information available to third parties will undoubtedly ease customers’ experience with safe payment services, the approach risks burdening banks, which will still bear the costs of maintaining payments accounts, but could be rendered into simple utilities. On the other hand, as observers and commentators have noted, banks could embrace the new opportunity to enhance their offerings to customers.

In detail, PSD2 has broadened the scope of the EU payments regulatory regime, which now extends to so-called "payment initiation service providers" (PISPs) and "account information service providers" (AISPs). Increases in territorial scope also extend the transparency rules of PSD2 to payment transactions in which one party is not in the European Union or in the European Economic Area (also known as "one-leg-out," or OLO transactions).[5] Significant changes have also been made to the "limited network" and "added value" exemptions that existed in the first Payment Services Directive (PSD1).[6] As for the controversial issue of the commercial agent exemption, consideration n. 11 of PSD2 tries to clarify that such exclusion should apply when agents act only on behalf of the payer or only on behalf of the payee, regardless of whether or not the agents are in possession of clients' funds. In particular, in the event these agents act as intermediaries on behalf of both the payer and the payee — such as certain online marketplace and e-commerce platforms — the agents should be excluded from the application of the Directive only if they do not, at any time, enter into possession or control of clients' funds. However, since the issue is addressed only in a consideration of the Directive and not in the regulatory provision itself, many fear that Member States might not take the issue into account.

In light of the increased attention the new actors of the payment services industry are receiving from regulators, the revisited framework introduces two new forms of payment services under Annex 1: the PISP[7] and the AISP[8] (also called third-party payments providers, hereinafter collectively the TPPs).[9] In general terms, the payment initiation services provider is a third party acting between the payee and its online bank account by prompting the payment in favor of a third-party beneficiary. The account information provider is a third party that organizes and supplies information to users based on their bank account (or accounts) through an online platform after their bank grants the third party online access. Such access is strictly limited, however, to the organization and rationalization of the information on the bank account, and does not grant any operational right to the account information provider.

The general rules have also increased the information obligations of the payment service providers in order to obtain authorization to operate from the competent authority. A new requirement was brought with the provision of a register to be held by the EBA.[10] In regards to competent authorities and supervision, the EBA has been mandated to draft the guidelines that will regulate the exercise of the freedom of establishment, as well as the provision of services.[11] The new directive has also introduced notification duties for the application of the exemptions.[12] Furthermore, the transparency of terms and conditions as well as the information requirements are now also applied to the TPPs.[13]

In respect to payment initiation services, the banks and other payment service providers will grant access to their customers' accounts to facilitate transactions.[14] This rule, the so-called "open access" rule or "XS2A," is one of the most important aspects of PSD2 because it will induce banks to allow access via APIs to their customer accounts upon the customers' authorization. At the same time, the initiation service providers are burdened with increased security obligations and liabilities in case of unauthorized or defective execution of payment transactions.[15] In particular, PSD2 provides new stricter requirements relating to customer authentication.[16] However, pursuant to the final draft of the RTS such requirements will not apply to, *inter alia*, "low risk transactions" for payments under €500 and to "unattended terminals" used for transport or parking fares.[17]

In relation to account information services, the new framework requires payment service providers to grant access to the accounts managed on behalf of a customer if the customer has given "explicit consent" to the PISP.[18] Account information services providers are also subject to the new security obligations.

In the context of the section relating to rights and obligations, the regime for allocating the liability between a TPP and other payment service providers[19] merits attention. The new debated liability regime

provides that in the case of an unauthorized payment made through an initiation payment provider, the account servicing payment service provider (ASPSP)[20] will be liable to reimburse the user, but then the ASPSP will have a remedy against the TPP.

Finally, the new rules also include transparency obligations over account services and charges, reporting obligations and complaint procedures for consumers.

Under these new rules, the consumers will theoretically benefit from receiving economic benefits, increased consumer rights and stronger payment security.[21]

The next *Client Alert* in this series will discuss the main criticisms arising from the more problematic provisions of PSD2, including *inter alia*, those regarding security and authentications,[22] and the related new provisions contained in the final RTS; the liability regime in case of unauthorized or defective payments; and the rules for OLO transactions.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Filippo Benintendi
filippo.benintendi@lw.com
+39.02.3046.2072
Milan

Christian F. McDermott
christian.mcdermott@lw.com
+44.20.7710.1198
London

You Might Also Be Interested In:

FCA Launches Discussion on Distributed Ledger Technology

What Do the SEC's Recent Bitcoin Disapproval Orders Really Mean for Investors?

Senior MP Calls for Regulatory Crackdown on Banks' IT Systems: 3 Things You Can Do to Prepare

---

[1] This *Client Alert Commentary* is in part based on the unpublished summative essay written by the author for the London School of Economics with the title 'The Payment Service Directive 2 and the banking system: "if we want things to stay as they are, things will have to change"' (Master of Laws, London School of Economics 2016).

[2] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (hereinafter: Payment Services Directive 2 or PSD2).

[3] For further information, see European Banking Authority, 'Final Report: Regulatory Technical Standards on strong customer authentication and common and secure communication under PSD2' (23 February 2017) available at https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf.

[4] The trend in the market for payment services is clear: transactions are generally moving away from cash towards mobile and internet payment methods. Against this backdrop, deficiencies were identified in the Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319 of 5 December 2007, 1-36 (PSD1), specifically in relation to keeping pace with technological evolution and allowing fair protection to all stakeholders without limiting innovation. In particular, the uncertainty created by the broad wording used in PSD1 as well as the proliferation of new payment systems and market players, among other factors, were not creating any harmonization but were instead fueling the fragmentation of the EU market of payment services. For further details, see European Commission, 'Report on the application of Directive 2007/64/EC on payment services in the internal market and on Regulation 924/2009 on cross-border payments in the Community' (2013) COM(2013) 549 final, 274 ff. Furthermore, in 2012, the European Commission in European Commission, 'Towards an integrated European market for card, internet and mobile payments' (Green Paper) COM (2011) 941 final, 3, made an assessment on the status of the European payment market stating that "payments have been identified as one of the main barriers to the future growth of e-commerce." In particular, the main obstacles were found to be the variety of payment methods in the European Union, the price of payments for consumers and businesses, and the payment security. The European body also acknowledged that the legal framework was disharmonized, the cross-border landscape was "fragmented" and the e-payment schemes were mainly confined within the domestic borders of the Member States. Moreover, the implementation of the exemptions of certain payment-related activities from the scope of the Directive proved to be disharmonized across the Member States, thus resulting in "regulatory arbitrage and legal uncertainty." The PSD2 came into force on 13 January 2016 with the very purpose of tackling these deficiencies. In fact, with this new text, the European lawmakers tried to disruptively reframe the regulatory landscape of the electronic payment industry by taking into account the ever-changing identity of the players, of the platforms, and of the devices involved, with the goal of making the payments services arena more innovative, competitive, and secure. While the road to the national transposition is still a long way ahead (EU Member States will have until 13 January 2018 to implement the new rules and replace the framework provided under PSD1), on 23 February 2017, with a delay of more than one month caused by the unusually high number of requests for clarification and concerns following the Consultation Paper issued last August, the EBA published the final draft of the RTS that payment service providers will be required to adhere to in order to meet the PDS2's stringent authentication requirements. The final draft RTS will be submitted to the Commission for adoption, following which the RTS will be subject to scrutiny by the European Parliament and the Council before being published in the Official Journal of the European Union in November 2018 at the earliest.

[5] Art 1-2 PSD2. See also Peggy Valcke and others, 'The Evolution of Third Party Payment Providers and Cryptocurrencies Under the EU's Upcoming PSD2 and AMLD4' (September 23, 2015) SWIFT Institute Working Paper No. 2015-001, 13. Available at http://ssrn.com/abstract=2665973 accessed 12 October 2016, 6.

[6] Art 3 PSD2. The limited network refers to those networks based on the use, among others, of electronic vouchers, loyalty schemes, fuel and membership cards, and cards for public transportation. The expansion of such networks has urged the European Commission to tighten the rules on such payment methods.

[7] A payment initiation service provider (or PISP) is a firm that can initiate payment transactions. In practice, upon request of an account holder, the PISP can take the money from the account and send it to another account.

[8] An account information service provider is a firm that connects to a bank account and retrieves information from it. A typical example would be a third-party personal and household budgeting service which organizes the information from the bank account, but does not initiate any payment transaction.

[9] Peggy Valcke and others (n. 5) 13. The European Commission observes in their Green Paper that the other types of e-payments are usually made in one of the following ways: (i) via a remote payment card transaction through the internet or (ii) through e-payment providers with which consumer has an account that has been funded by using "traditional" payment methods (for example bank transfers or credit card payments). See European Commission (n. 4) 4.

[10] Art 15 PSD2.

[11] Arts 22-31 PSD2.

[12] Art 32-34 PSD2.

[13] Art 30-60 PSD2.

[14] Art 66 PSD2.

[15] Art 90 PSD2.

[16] The European Commission in European Commission (n. 4) 5 explains the new security requirements set forth under art 97 PSD2 as follows: "the payment service providers will be obliged to apply so-called strong customer authentication (SCA) when a payer initiates an electronic payment transaction. Strong customer authentication is an authentication process that validates the

identity of the user of a payment service or of the payment transaction (more specifically, whether the use of a payment instrument is authorised). Strong customer authentication is based on the use of two or more elements categorised as knowledge (something only the user knows, e.g. a password or a PIN), possession (something only the user possesses, e.g. the card or an authentication code generating device) and inherence (something the user is, e.g. the use of a fingerprint or voice recognition) to validate the user or the transaction. These elements are independent (the breach of one element does not compromise the reliability of the others) and designed in such a way as to protect the confidentiality of the authentication data. For remote transactions, such as online payments, the security requirements go even further, requiring a dynamic link to the amount of the transaction and the account of the payee, to further protect the user by minimizing the risks in case of mistakes or fraudulent attacks."

[17] In particular, the final draft of the RTS introduced a new section allowing PISPs to use a "transaction risk analysis" to identify the transactions, under €500 each, with a low level of risk and be exempt from the strong customer authentication requirement. However, PISPs need to notify the regulator of their intention of using this analysis and show fraud levels within the rates mandated by the RTS. Further exemptions include, the exemption for "unattended terminals" used for transport and parking fees and an increase in the threshold for remote transactions from €10 to €40. On the contrary, the final RTS confirmed no exemptions for corporate payments.

[18] Art 67 PSD2.

[19] Art 73 PSD2.

[20] Under the terminology of PSD2 the ASPSP are those who maintain the payment accounts, *i.e.* the banks. For the provision see Art. 97(5) PSD2.

[21] For more details see European Commission (n. 4) 2.

[22] The European Banking Federation has condemned the overall result of the harmonized framework by officially saying that the framework agreement will be "to the detriment of European consumers and the necessary protection to their bank accounts. The PSD2 framework is already partly obsolete and above all harmful as it requires the sharing of bank access codes with non-bank providers." See European Banking Federation, 'EBF statement on EU payment services agreement' (EBF-FBE website, 6 May 2015) available at http://www.ebf-fbe.eu/wp-content/uploads/2015/05/EBF_014722-PSD2-trilogue-outcome-EBF-statement.pdf accessed 12 October 2016.