EU Payment Services Directive II Introduces Broader, More Stringent Regulation of Payment Services

Introduction

Two years after the European Commission’s original legislative proposal in July 2013,¹ the Payment Services Directive II (PSD II)² has now completed its legislative journey, having been approved by the EU Council on November 16, 2015 and published in the Official Journal on December 23, 2015. Member States must now start the process of implementing PSD II into national law. Such national laws must be effective no later than January 13, 2018. PSD II is meant to update the first Payment Services Directive (PSD I),³ which currently governs the regulatory regime for payment services in the EU. It brings into scope payment service providers (PSPs) that were previously unregulated and raises conduct of business standards in certain key areas, including security requirements. This Update sets out in further detail some of the key changes being introduced.

Scope

Territorial Scope

PSD I broadly applies only to intra-EU payments involving EEA currencies (e.g., euro or sterling). The revised directive, however, extends this scope for certain transactions. The main PSD II provisions affected by this extension in scope are those concerning conduct of business requirements, e.g., the mandatory disclosure of certain information to payment service users (under Title III) and those creating specific rights and obligations (under Title IV). As before, for payment transactions taking place wholly within the EU and in an EEA currency, all of these conduct of business requirements apply; for transactions where both the payer’s and payee’s PSPs are, or the sole PSP is, located in the EU, but a non-EEA currency is involved, a more limited set of provisions applies; and where the payment transaction involves any currency, but only one PSP is located within the EU, other (more limited) provisions apply. Given this broader territorial reach, firms will need to update their customer documentation, in addition to systems and processes, to apply the conduct of business rules to a broader range of transactions.

³ Directive on payment services in the internal market (Directive 2007/64/EC).
Negative Scope

The revised directive carries forward most of the exemptions that are available under the current regime. Payment transactions carried out within a payment or securities settlement system, transactions related to investment services (e.g., payments of dividend income), and services provided by technical service providers (e.g., data processing) all remain outside the scope of PSD II, as was the case under PSD I. However, a number of exemptions which are currently available to firms have been revised.

(a) Commercial agent exemption: PSD I contained a ‘commercial agent’ exemption, which allowed for PSPs to remain out of scope when acting as commercial agents channeling payment transactions from a payer to a payee. This exemption has now been limited under PSD II so as to apply only where a PSP is acting solely for the payer or the payee but not both. Thus, a PSP wanting to benefit from this exemption can only be an agent of either the payer or the payee.

The Commission’s stated rationale for narrowing the commercial agent exemption is the need to address the lack of uniformity in its current application among Member States, as well as an attempt to minimize the distortion of competition in the payments market. The impact of this narrowing of the current exemption is that more e-commerce marketplace business models will likely fall within the scope of EU payments regulation, and firms which currently rely on this exemption may no longer be able to do so under PSD II, forcing such firms to either apply for authorization or change their business models.

(b) Limited network exemption: Under PSD I, certain payment services currently qualify for the ‘limited network’ exemption, in cases where a payment instrument (e.g., a card) can only be used to purchase a limited range of goods or services, or within a limited network of merchants. PSD II refines this exemption to include specific payment instruments that can be used: “only to acquire a very limited range of goods or services” (emphasis added), for purchases from the issuer’s limited network or other network of service providers, or in a single Member State for social or tax purposes. It is therefore expected that store/membership cards and pre-paid cards which can be used by more than one retailer may be affected by this narrowing. National Competent Authorities (NCAs) will also need to be notified of firms wishing to benefit from the limited network exemption should their total exempted transaction values in the preceding 12 months reach a threshold of €1 million.

While it remains unclear what the precise parameters applicable to a “very limited” range of goods would be, this restriction of the limited network exemption will generally mean that card systems such as electronic vouchers redeemable at multiple merchants are likely to attract regulatory scrutiny if they cannot be used in very limited circumstances.

(c) Telco/digital device exemption: Under PSD I, a telecommunications (‘telco’), digital or IT operator can benefit from the ‘download exemption’ for payment transactions in respect of certain digital content (e.g., ringtones, apps and games). The exemption for low value payments for such digital content has been narrowed under PSD II to apply only where individual payments for ancillary services do not exceed €50 for individual transactions, subject to an overall cap of €300 per month.

For firms wishing to remain within this exemption, system changes will have to be made to enable digital providers to monitor the €50/€300 threshold.
(d) **Cash withdrawal services exemption:** The current exemption for cash withdrawal services provided by independent operators of ATMs under PSD I has now been amended to include a new requirement for mandatory disclosure of fees associated with ATM withdrawals. As before, an ATM provider wishing to avail itself of this exemption cannot conduct any other regulated payment services.

**Regulated Payment Services**

**Payment Service Providers**

The range of entities falling within the definition of “payment service provider” remains broadly unchanged under PSD II: credit institutions, e-money institutions and payment institutions, among other types of entities, will continue to be deemed PSPs. Likewise, the services that constitute “payment services” and thus are regulated under the directive remain largely the same. However, two new services have been brought into scope.

**New Regulated Payment Services**

In an effort to keep pace with innovations in the payments industry, PSD II has brought into scope the following types of non-execution third party payment service providers (TPPs), which were previously unregulated:

(a) **payment initiation services providers** (PISPs), which provide services to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider; and

(b) **account information services providers** (AISPs), which provide consolidated information on one or more payment accounts held by payment service users with more than one PSP (typically via the online channel). AISPs will be allowed to provide services on a cross-border basis, thus benefiting from the passporting rules.

Note that as TPPs will not be allowed to come into possession of funds, the ‘technical service provider’ exemption under Art. 3(j) of PSD II has been clarified to specifically exclude these new TPPs. Alongside the introduction of new regulated services, a key driver of the reforms introduced under PSD II has been the desire to open up access to payment account information to third parties. Licensed TPPs will in future have access rights to bank accounts (once they are granted “explicit consent” by the payment service user) and so will be able to check availability of funds and initiate payment transactions (e.g., a debit from a current account), as well as provide more generic account information services.

**Access Rights of TPPs**

Importantly, PSPs will be barred from denying TPPs access to bank accounts, and account servicing PSPs will be required to treat payment orders (in the case of PISPs) and data requests (in the case of AISPs) without discrimination, e.g., by applying additional charges, or treating them with lower priority in terms of execution/timing. PSPs will be able to deny access, however, where suspicion of fraudulent or unauthorized activity can be “objectively justified and duly evidenced.”

These two new regulated entities – PISPs and AISPs – will be required to hold either professional indemnity insurance or a comparable guarantee. New market entrants may therefore find this initial requirement a potential barrier to entry.
Impact

A range of business models will newly be caught under the new rules governing TPPs. Firms which currently provide payment initiation services or account information services will in future be required to be authorized and supervised as payment institutions, albeit just for these limited activities. Data protection and security requirements that are currently applicable to ‘traditional’ forms of payment service providers will also be applicable to TPPs. Also, any TPP which was providing payment initiation or account information services before January 12, 2016 may continue to provide such services on an unregulated basis until January 2018.

As to the new provisions on non-discriminatory access for TPPs, account servicing PSPs will have to ensure that their current systems do not put PISPs and AISPs at a disadvantage in terms of execution times. They will also need to have systems in place to “communicate securely with” PISPs and AISPs. New technical interfaces and online authentication procedures will therefore need to be developed, in addition to adapting to a new environment where an intermediary can now sit between their customers and themselves. Robust documentation clearly delineating the liability of PISPs, AISPs and PSPs in their relationships will need to be developed.

Regulation of Payment Service Providers

Authorization of Payment Institutions

Once PSD II comes into force, payment institutions will be subject to broader authorization requirements, including: documentary evidence of procedures in place for security risk management and dispute resolution; business continuity arrangements; a security policy document (including data protection considerations); information on the use of statistical data on performance, transactions and fraud; and procedures for monitoring agents and branches. Firms which are already authorized payment institutions should consider updating their compliance manuals to fulfill the ongoing threshold conditions under PSD II. Newly regulated firms will need to devise their own compliance documentation.

Although the regulatory regime governing the use of agents remains largely unchanged under PSD II, payment institutions will be under a new obligation to inform NCAs of any “material changes” to their agents’ money laundering internal controls. Payment institutions wishing to provide payment services on a cross-border basis via an agent will be subject to a largely unchanged application process for a passport. However, under the new regime, NCAs in the host Member States will additionally have the power to request periodic reports on the activities carried out in their territories and require that a central contact point in their territory be established.

EU Payment Institution Register

A new central register for payment institutions will need to be developed by the EBA, who will need to make it publicly available, searchable, and free of charge. Firms will therefore need to ensure that they provide up-to-date information to the EBA for the purposes of the register.

Access to Payment Systems

PSD II preserves the current protections against discrimination for all PSPs in terms of their access to payment systems. This includes the rights of payment institutions and credit institutions to use the services of the payment systems’ technical infrastructure.
Information and Conduct of Business Requirements

Application

Many of the disclosure and conduct of business rules under Titles III and IV of PSD I have been carried over to PSD II. As with PSD I, under the new regime, parties to a payment transaction may opt out of the Title III provisions, which govern transparency and information requirements, where the payment service user is not a consumer. The same applies to certain conduct of business requirements under Title IV. Member States may also continue by way of derogation to treat micro-enterprises as consumers.

In addition, to reflect the inclusion of PISPs within the regulatory perimeter under PSD II, new disclosure provisions for PISPs are introduced for single payment transactions. These include: (i) a requirement to provide the identity of the PISP prior to the initiation of a payment transaction; and (ii) other transparency requirements once the payment order has been initiated.

Termination Rights

Termination of a framework contract is free of charge except where it has been in force for less than six months, as opposed to 12 months which is currently the case under PSD I.

Liability Provisions

PSD II reduces a customer’s liability for unauthorized transactions to €50 (as compared to €150 under PSD I) and imposes obligations on PSPs to refund erroneous transactions by the end of the following business day, except where fraud is suspected. Specific liability provisions have also been set down for PISPs. Firms will need to review terms and conditions/customer disclosure documents to ensure consistency in liability provisions and associated protection.

Complaints and ADR Procedures

Formal complaint handling procedures for PSPs have been introduced under PSD II: they will be required to reply to complaints within 15 business days (whereas there was no explicit timescale under PSD I) and comply with further rules on escalation procedures. Member States will have discretion to goldplate these dispute resolution procedures to the benefit of payment service users.

The European Commission is to publish an electronic leaflet explaining the rights of payment users, and PSPs must ensure that this is made available at no charge in an accessible manner to customers, including through appropriate alternative means for persons with disabilities, if required.

Penalties

While PSD II has maintained the broad discretion for Member States to set penalties as was the case under PSD I, the revised directive introduces a new public disclosure power for competent authorities, except where such disclosure would jeopardize the financial markets or cause disproportionate damage to the parties involved.

Security Measures

One of the most important developments under the revised directive is the introduction of a swathe of new security requirements for PSPs for the initiation and processing of electronic payments and the protection of
consumers’ financial data. They will be required to apply “strong customer authentication” when a payer accesses its payment account online or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses (e.g., mobile payments). In addition, where a payer initiates electronic payment transactions, the authentication procedure must also include elements which dynamically link the transaction to a specific amount and a specific payee.

In future, PSPs will also be required to provide an annual overview of risks faced by its payment services and of the adequacy of risk mitigation measures. Where a “major operational or security incident” occurs, PSPs will be required to notify the relevant NCA “without undue delay.” Once an NCA has notified the European Banking Authority (EBA) and European Central Bank (ECB) of such incidents, an ensuing assessment by both bodies will determine whether other NCAs need to be notified. The general point of this reporting chain is for relevant authorities to understand the wider impacts on the EU payments system and act accordingly. PSPs are also required to notify customers without undue delay if a security incident might negatively impact their financial interests. A new requirement for statistical data on fraud relating to different means of payment has also been introduced.

Note that, in contrast to the other PSD II mandates which must be implemented 24 months after entry into force of the directive, the technical standards on strong customer authentication and secure communication will apply at a later date, which is likely to be no earlier than the end of 2018. It should also be borne in mind that the EBA introduced new guidelines for security of payment transactions in August 2015. Although this guidance has not been fully introduced in every Member State (and indeed the UK Financial Conduct Authority has chosen not to introduce new rules to reflect this guidance), many firms are likely to have made some changes reflecting these requirements.

To some extent, the premature publication of the EBA security guidelines may force firms to undertake a two-phase review of their payments security policies and procedures. This is the case, for example, in countries which have mandated compliance with the EBA guidelines.\(^4\) More broadly, once PSD II is implemented, firms will be required to amend current information security policies and procedures to reflect these changes, new systems for customer authentication may need to be developed, and reporting mechanisms will also need to be reviewed. Governance procedures will also need to reflect these changes.

**Future Regulatory Technical Standards**

The final text confirms that the EBA is to develop regulatory technical standards (RTSs) and/or guidelines on:

(a) information to be provided to the competent authorities in an application for authorization, by January 3, 2017;

(b) authentication and communication requirements (taking into account the privacy dimension), by January 13, 2017;

(c) the development, operation and maintenance of the electronic central register and on related access, by January 13, 2017;

\(^4\) For a list of countries which comply (or intend to comply) with the EBA guidelines as at July 31, 2015, see [https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+Compliance+Table-GL+security+of+internet+payments.pdf](https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+Compliance+Table-GL+security+of+internet+payments.pdf).
(d) the appointment of a central contact point (under passporting requirements), and the functions of those contact points, by January 13, 2017;

(e) operational and security risks, by July 13, 2017; and

(f) the framework for cooperation and data exchange between Member States, by January 13, 2018.

Conclusion

Clearly, the revised regime for regulating payment services in the EU introduces a swathe of new requirements both for firms which are already regulated as payment institutions, and for those who will be newly regulated. Affected firms will benefit from early planning to update relevant systems and procedures, train staff and develop risk identification and mitigation strategies in order to realize the Commission’s stated intention of raising standards in the payments industry.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work, or

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Casanova</td>
<td>Partner</td>
<td>+44 20 7360 3739 <a href="mailto:jcasanova@sidley.com">jcasanova@sidley.com</a></td>
</tr>
<tr>
<td>William Long</td>
<td>Partner</td>
<td>+44 20 7360 2061 <a href="mailto:wlong@sidley.com">wlong@sidley.com</a></td>
</tr>
<tr>
<td>Max Savoie</td>
<td>Associate</td>
<td>+44 20 7360 3682 <a href="mailto:msavoie@sidley.com">msavoie@sidley.com</a></td>
</tr>
<tr>
<td>Grace Wyatt</td>
<td>Associate</td>
<td>+44 20 7360 2055 <a href="mailto:gwyatt@sidley.com">gwyatt@sidley.com</a></td>
</tr>
</tbody>
</table>

Sidley Banking and Financial Services Practice

The Banking and Financial Services Practice group offers counseling, transaction and litigation services to domestic and non-U.S. financial institutions and their holding companies, as well as securities, insurance, finance, mortgage, and diversified companies that provide financial services. We also represent all sectors of the payments industry, including payment networks and processors, money transmitters, and payors and payees in various systems. We represent financial services clients before the U.S. Department of the Treasury, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau and state regulatory agencies, as well as financial services regulators in other jurisdictions where we have offices. In addition, we represent clients before the United States Supreme Court, other federal courts and state courts.

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.