Payment Services Directive II

Introduction

The payment services industry has undergone profound change since the landmark Payment Services Directive ("PSD 1") was introduced in 2007. Developments in technology and the emergence of new payment services providers have fundamentally altered the market landscape. The new Payment Services Directive II ("PSD 2") is designed to update the rules in respect of payment services, to reflect and regulate aspects of these recent developments.

PSD 2 must be transposed into Irish law by 13 January 2018. From a practical viewpoint, PSD 2 widens the scope of the original rules, covering new services and market operators. While much of the framework of PSD 1 has been retained, an additional layer of obligations will be placed on Payment Service Providers ("PSPs") under the new legislation. This will require PSPs to review their internal procedures and systems to take account of and ensure compliance with PSD 2.

1 Key New Features of PSD 2

1.1 Extension of Scope of Transactions Covered

The original PSD 1 imposed conduct of business rules only on intra-European Union transactions. PSD 2 significantly extends the range of transactions governed by the rules. These conduct rules apply on a tiered system. At the top tier, the most extensive rules apply to payment transactions in the currency of a Member State, where both the payer’s and payee’s PSP are located within the European Union ("EU").

In the middle tier, a less extensive set of rules applies to payment transactions in a non-Member State currency, where both the payee’s PSP and the payer’s PSP are located within the EU.

In the bottom tier, a much less extensive regime applies to payment transactions in all currencies where only one of the PSPs is located within the EU, in respect of those transactions carried out in the EU.

Therefore, even those transactions where only one element or party is based within the EU, now fall within the regulatory net where previously they incurred no obligations. As a consequence, detailed rules in relation to transparency, provision of information, and conduct of business must be implemented in the way they offer their payment services.

1.2 Revision and Reduction of Exemptions Provided to PSPs

Most exemptions that were available under PSD 1 have been retained in the new legislation. However, certain exemptions that previously applied to market operators have been revised and narrowed in scope, in particular:
- **Commercial Agent Exemption:** Under PSD 1, certain PSPs could avoid authorisation requirements when acting as a ‘commercial agent’ in routing payment transactions between a payer and payee. However, under the new legislation, this exemption will only be applicable when acting for either the payer or payee; and

- **Limited Network Exemption:** Under the previous legislation, this exemption applied where a payment instrument, such as a card, only allowed the purchase of a limited range of goods. PSD 2 refines this exemption. The exemption will only apply in future where the instrument allows merely the purchase of goods and services in a specific retailer or retail chain, or in a single member state. There is a lack of clarity in the legislation; however, store cards and pre-paid cards that can be used at multiple retailers may now come within the ambit of the new Directive.

### 1.3 Extension of Scope to Third Party Payment Service Providers

PSD 2 retains the same categories of PSPs as applied under the original Directive. However, in an effort to regulate new market operators, PSD 2 brings within its scope certain third party payment providers that were previously unregulated.

The first such category is a Payment Initiation Service Provider (‘**PISP**’). This relates to a party which initiates a payment order requested by the customer, in relation to the customer’s account held at a PSP. The most common example arises in online banking. In such a situation, the customer shares his security credentials with the bank, but does so via a third party software provider. Notably, the PISP does not manage customer funds at any stage of the transaction, yet will be the subject of regulatory rules for the first time under PSD 2.

The second new category is an Account Information Services Provider (‘**AISP**’). This relates to a party which provides consolidated information on payment accounts held by customers with more than one PSP, commonly known as ‘account aggregators’.

### 1.4 Effect of Regulation of Third Party Payment Service Providers

Those market operators whose activity falls within the definition of a PISP above will now be obliged to seek authorisation, and face ongoing supervision, in a broadly similar manner to PSPs. Data protection and security requirements that presently apply to PSPs, will also apply to these third party providers (albeit in a less stringent manner) in future. AISP will not need to be authorised, but will need to register, with their national competent authority.

The inclusion of third party actors also has implications for existing PSPs. PSPs must provide third party payment providers with customer account information and access to the account itself, provided the customer has consented to this. In essence, the PSP must treat third party providers’ payments in the same way as if the request came from the customer directly. A practical effect is that a PSP cannot impose extra cost constraints on third party providers.
1.5 **Enhanced Authorisation Requirements**

Under PSD 2, the authorisation requirements under the original Directive are retained. However, certain additional documentation must be submitted to the relevant national authority. A security policy document must now be maintained by the PSP, containing a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified. Other additional requirements involve producing a description of business continuity arrangements, together with a clear identification of the critical operations, contingency plans, and management systems in respect of a security incident.

1.6 **Security Authentication and Security Management**

A key trend in regulatory policy in recent times is the focus on cyber security. The European Banking Authority (“EBA”), which is a form of EU-wide bank regulator, issued “Guidelines on the Security of Internet Payments” in June 2015, designed to improve the security of online payments. PSD 2 follows this trend by providing a legislative basis for cyber security.

Where a customer accessing an online account initiates a payment transaction, PSD 2 requires PSPs to apply “strong customer authentication” procedures. The exact requirements of such procedures will be elaborated by the EBA. An emphasis is also placed on security breaches. A PSP must inform the national competent authority if it experiences a “major operational or security incident”. It must also inform the customer if the incident “has or may have an impact on the financial interests of its payment service users.”

2 **Areas of PSD II Requiring Further Clarification**

2.1 **Regulatory Technical Standards on Security Requirements**

PSD 2 requires the EBA to publish detailed rules on security requirements in the form of regulatory technical standards (“RTS”). This will provide further detail for Obliged Entities on the exact implications of “strong customer authentication” referred to above. Additional information is also expected on the security measures to be taken to protect the confidentiality and integrity of the customer’s personalised security credentials.

2.2 **Regulatory Technical Standards on Communication**

RTS will also be made available on the requirements for secure standards of communication for the purpose of identifying customers, and related authentication, notification, and information distribution. In this regard, further guidance is required on the privacy aspects of such communications, in order to identify the associated risks and remedies that could be put in place to minimise threats to data protection.
Preparatory Actions for Businesses

In advance of PSD 2’s implementation in January 2018, businesses should consider reviewing how they provide their payment processing services and amending them to comply with the increased standards demanded by the new Directive:

- Market operators who benefitted from exemptions under PSD 1 may now find that they no longer satisfy the narrower exemptions under the new legislation, particularly those businesses operating store cards and pre-paid card systems. Such entities may require to be authorised as PSPs, and comply with the attendant rules;

- Market operators who currently provide payment initiation or account information services will soon be required to be authorised for the first time. This will entail significant data protection and security requirements to be implemented across internal systems to ensure compliance with PSD 2;

- Traditional and existing PSPs will need to review internal software and order processing to ensure that PISPs and AISPs are not subject to additional barriers;

- Traditional PSPs should be advised to enter into contracts with their third party providers, formalising and setting the parameters of their relationship;

- An overhaul of compliance policies may be necessary to comply with the increased burden of authorisation requirements mandated under PSD 2. Businesses will be required to submit detailed authorisation materials to the national competent authority in advance of 13 July 2018 (the end of the transitional period) in order to gain authorisation under PSD 2; and

- In particular, consumer authentication procedures must be implemented, with PSPs required to provide a yearly assessment of its risk measures to the national regulator.

How Matheson Can Help

All Obliged Entities will be advised to review their communication and security frameworks to assess compliance with the expectations of the impending PSD 2 regime. Even if only limited amendments are required, firms will be in a better position having completed a comprehensive review, should the Central Bank of Ireland undertake an inspection in their firm as they will be able to demonstrate that they took action to assess their compliance with same.

We provide a number of services to assist clients in the area of PSD2, including:

- Reviewing policies and procedures and undertaking a full gap analysis against the expectations of PSD 2;

- Providing annual and ad hoc update training to relevant staff and senior management, to ensure any regulatory or legal changes are notified to the relevant staff and senior management in a timely manner;
- Undertaking a mock-inspection to assess the extent of compliance, in practice, with the firm’s own internal policies and procedures in relation to PSD 2; and
- Assisting new and existing PSPs in authorisation applications and advice on ongoing supervision by the Central Bank in respect of PSD 2.

Contacts

Joe Beashel  
Partner  
Tel: +353 1 232 2101  
E: joe.beashel@matheson.com

Edmond O’Hanlon  
Associate  
Tel: +353 1 232 2249  
E: Edmond.ohanlon@matheson.com

Colm Dawson  
Tel: +353 1 232 2162  
E: colm.dawson@matheson.com