June 19, 2015

Background

The first Payment Services Directive (PSD1) was proposed by the European Commission in 2005, and adopted by the European Parliament and Council in 2007.

Since then, the retail payments market has grown significantly, and new payment services have been developed. However, the payments market is still fragmented along national borders; some payment products and services are out of scope, and some of PSD1 is "*too ambiguous, too general or simply outdated*". This has resulted in "*legal uncertainty, potential security risks in the payment chain and a lack of consumer protection in certain areas*". It has also made it difficult for innovative and easy to use digital payment services to "*take off*".

The European Commission therefore proposed "*new rules … to close the regulatory gaps[; provide] more legal clarity[; ensure] a consistent application of the legislative framework across the Union[; facilitate] new means of payment …and [ensure] a high level of consumer protection … across … the Union*".[1]

For the purposes of this client alert we have assumed that, if these new rules are made, they will be in materially the same form as the final compromise text of the proposed Second Payment Services Directive (PSD 2), published by the European Council on 2 June 2015. If the new rules are made, PSD2 will repeal and replace PSD1. Many of the provisions in PSD2 will be materially the same as those in PSD1, but some will require more than they require today, and others will be entirely new. For brevity and simplicity, this client alert is concerned only with the most significant differences between PSD1 and PSD2. We have not used it to summarise the existing regime.

Scope

PSD1 applies to "*payment services provided within the Community*". However, PSD1 Title III (Transparency of conditions and information requirements for payment services),[2] and PSD1 Title IV (Rights and obligations in relation to the provision and use of payment services),[3] only apply:[4]

- Where both the payer's payment services provider (PSP) and the payee's PSP are, or the sole PSP is, in the EU; and
- To payment services that use the Euro or the currency of an EU Member State outside the Eurozone.

PSD2 will apply more widely because (for example):

- It will also apply to:
  - The carrying out of two new payment services (payment initiation services, and account information services, as to which, see below);[5] and
  - Payment transactions initiated by the payee, the payer *and* those initiated on the payer's behalf;[6] and
- Most of PSD2 Title III[7] and PSD2 Title IV[8] will also apply[9] to:
  - Transactions in *any currency*, if both the payer's PSP and the payee's PSP, or the sole PSP, are located in the Union; and

- Payment transactions where only one of the PSPs is in the EU, in respect of those parts of the payments transaction which are carried out in the EU (these arrangements are sometimes referred to as "*one leg out*" transactions).

Payment initiation services

Article 58 of PSD2 will require the EU Member States to:

- Ensure that payers have the right to use a payment initiation service provider (PISP) to obtain **payment initiation services**;
- Require the account servicing PSPs domiciled in their jurisdiction to:

  *"(a) provide facilities to **securely communicate** with [PISPs]in accordance with **article 87a, paragraph 1(d)**;*

  (b) immediately after the receipt of the payment order from a [PISP,] provide or make available all information on the initiation of the payment transaction... to the [PISP]; and

  *(c) treat payment orders transmitted through the services of a [PISP] without any discrimination **for other than objective reasons**, in particular in terms of timing, priority or charges vis-à-vis payment orders transmitted directly by the payer himself* and
- (When the payer gives its **explicit consent** for a payment to be executed in accordance with article 57), require their account servicing PSPs:

  "(-a) not to hold … the payer's funds in connection with the provision of the payment initiation service;

  (a) to ensure that the personalised security credentials of the payment service user, are not, with the exception of the user and the issuer of the personalised credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

  (aa) to ensure that any other information about the payment service user, obtained when providing payment initiation services, is only provided to the payee and only with the payment service user's explicit consent;

  *(b) every time a payment is initiated, to identify itself towards the account servicing [PSP] of the account owner and communicate with the account servicing [PSP], the payer and the payee in a secure way, in accordance with **article 87a, paragraph 1(d)***

  (d) not to store sensitive payment data of the payment service user ;

  (da) not to request from the payment service user any data other than those necessary to provide the payment initiation service;

  (e) not to use, access and store any data for purposes other than for the provision of the payment initiation services;

  (f) not to modify the amount, the recipient or any other feature of the transaction".

For these purposes:

Authentication	is *"any procedure which allows the [PSP] to verify the identity of the payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials*" (see article 4(21) of PSD2);
A payment initiation service	is "*a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another [PSP]*" (see article 4(32) of PSD2);
Payment initiation services	"*play a part in e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the payer's bank in order to initiate internet payments on the basis of a credit transfer ... These services enable the [PISP] to provide comfort to a payee that the payment has been initiated. This aims at incentivising the payee to release the good [sic] or deliver the service without undue delay. These services… provide consumers with a possibility to shop online even if they do not possess payment cards …*." (see recital 18 to PSD2); and
A payment order	is "*any instruction by a payer or payee to his [PSP] requesting the execution of a payment transaction*" (see article 4(18) of PSD2).

However, PSD2 does not define or explain the terms:

Explicit consent	although article 57 provides that: "*(1) …a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the [PSP], after the execution of the payment transaction.* *(2) Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the [PSP]. Consent to execute a payment transaction may also be given via the payee or the [PISP]...* *(3) Consent may be withdrawn by the payer at any time...* *(4) The procedure for giving consent shall be agreed between the payer and the relevant [PSP]*";
Objective reasons or	

Securely communicate	although **article 87a, paragraph 1(d)** provides that: "*(1) [The European Banking Authority] shall...in close cooperation with the [European Central Bank], develop draft regulatory technical standards addressed to [PSPs] … specifying:* *(d) the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification and information between account servicing [PSPs], [PISPs], account information service providers, payers, payees and other payment service providers."*

Account information services

Article 59 of PSD2 will also require the EU Member States to make sure that payment service users have the right to use payment **account information services**. To facilitate this, articles 59(2) and (3) of PSD2 will require:

- The account information service provider (AISP):

  "(a) to provide services only based on the payment service user's explicit consent[as to which, see above];

  (aa) to ensure that the personalised security credentials of the payment service user, are not, with the exception of the user and the issuer of the personalised credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels;

  (b) for each communication session, identify itself towards the account servicing [PSP] of the payment service user and securely communicate with the account servicing [PSP] and the payment service user, in accordance with Article 87a, paragraph 1,(d)[as to which, see above];

  ([c]) to access only the information from designated payment accounts and associated payment transactions;

  *([d]) not to request **sensitive payment data** linked to the payment accounts;*

  ([e]) not to use, access and store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules"; and

- The account servicing PSP to:

  *"(a) to securely communicate with the [AISP], in accordance with **article 87a, paragraph 1,(d)**[as to which, see above]; and*

  (b) treat data requests transmitted through the services of an [AISP] without any discrimination for other than objective reasons [as to which, see above]".

However, "*An account servicing [PSP] may deny access to the payment account for an [AISP] or a [PISP] for objectively justified and duly evidenced reasons related to unauthorised or fraudulent access to the payment account…*" In such cases, *the account servicing [PSP] shall inform the payer of the denying access to the payment account and the reasons for it …, where possible, before the access is denied and at the latest immediately thereafter, unless giving such information would compromise objectively justified security reasons or is prohibited by [law]. The account servicing [PSP] shall allow access to the payment account once the reasons for denying access no longer exist*"[10].

For these purposes:

Account information services	are online services that "*provide consolidated information on one or more payment accounts held by the payment service user with one or more other [PSPs]*" (see article 4(33) of PSP2); and "…*These services provide the payment service user with aggregated online information on one or more payment accounts held with one or more other [PSPs] and accessed via online interfaces of the account servicing [PSP], thus enabling the payment service user to have an overall view of his financial situation* …" (see recital (18a) to PSD2); and
Sensitive payment data	means "*data, including personalised security credentials which allow control over the payment service user's account or can be used to carry out fraud*" (see article 4(22c) of PSD2). For the activities of [PISPs] and [AISPs], the name of the account owner and the account number do not constitute sensitive payment data.

Strong customer authentication

Under article 87 of PSD2, the EU Member States will be obliged to ensure that PSPs apply "***strong customer authentication*** *when the payer:(a) accesses his payment account on-line; (b) initiates an electronic* ***remote payment transaction****; [or] (c) carries out any action, through a remote channel, which may imply a risk of payment fraud or other abuses*".

Member States must also ensure that PSPs:

- Meet specific security requirements to *"protect the confidentiality and integrity of payment service users'* ***personalised security credentials"***; and
- (Where a payer initiates an electronic remote payment transaction) adopt "*strong customer authentication that shall include elements dynamically linking the transaction to a specific amount and a specific payee*".

Draft regulatory technical standards will be developed by the European Banking Authority and submitted to the Commission within 12 months of PSD2 entering into force that will specify:

"*(a) the requirements of the strong customer authentication procedure;*

(b) the exemptions to the application of [strong customer authentication];

(c) the requirements that technical security measures have to comply with … to protect the confidentiality and the integrity of the payment service users' personalised security credentials; and

(d) common and secure requirements for communication for the purpose of authentication, notification and information, as well as for implementation of security measures between account servicing [PSPs], [PISPs], [AISPs], payers and payees".

For these purposes:

Strong customer authentication	means "*an authentication based on the prompt use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is)…that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data*" (see article 4(22) of PSD2); and
Personalised security credentials	means *"personalised features provided by the [PSP] to a payment service user for the purposes of authentication*" (see article 4(22a) of PSD2).
Remote payment transaction	means "*a payment transaction initiated via internet or through a device that can be used for distance communication*"

Lost or stolen payment instruments and unauthorised payment transactions

Articles 61 to 66 of PSD2 set down the respective obligations of payment services users and PSPs in relation to payment instruments. A payment service user entitled to use a payment instrument will be obliged to "*use the payment instrument in accordance with [its] terms … [which] must be objective, non-discriminatory and proportionate [and] notify the [PSP]… on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorised use*".

A PSP issuing a payment instrument will be obliged to "*ensure that appropriate means are available at all times to enable the payment service user to make a notification [as described above, and]… provide the payer with an option to make a notification … **free of charge** and to charge, if at all, only replacement costs directly attributed to the payment instrument*".

PSD2 will continue to require the PSP to provide rectification to the payment service user if the payment service user "*notifies the [PSP] without undue delay on becoming aware of any unauthorised or incorrectly executed payment transactions giving rise to a claim*". However, it will also require that "*the credit value date for the payer's payment account … be no later than the [debit] date*" and that where a transaction is initiated through a PISP, "*the account servicing [PSP must] refund immediately... the amount of the unauthorised payment transaction*" before seeking compensation from the PISP if appropriate.

The payer may be obliged to pay up to a maximum of €50 (the equivalent amount under PSD1 is €150) for "*losses relating to any unauthorised payment transactions … resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument*".

Internal dispute resolution

PSD2 will require PSPs to maintain more robust and complete internal dispute resolution systems than PSD1 requires today. In particular, PSPs will be required to:

"(1) … put in place and apply adequate and effective complaint resolution procedures for the settlement of complaints of payment service users [which shall be] applied in every Member State where the [PSP] offers the payment services … and … available in

the official language or one of the official languages of the relevant Member State or in another language if agreed between the [PSP] and the payment service user.

(2)… make every possible effort to reply … to the payment service users' complaints [addressing] all points raised … at the latest within 15 business days of receipt of the complaint. In exceptional situations, if the answer cannot be given within 15 business days for reasons beyond the control of the [PSP], it shall...send a holding reply clearly indicating the reasons for delay … and specifying the deadline by which the payment service user will receive the final reply. That deadline may not, in any case, exceed another 35 business days" (see article 90 of PSD2).

A maximum harmonising directive

PSD2 will be a maximum harmonising directive. The European Member States will not therefore be able to require any more or any less of the firms established in their jurisdictions than PSD2 itself will require. Article 95 of PSD2 lists a small number of exemptions to this rule.

Implementation and next steps

The final compromise text of PSD2 was agreed at a trilogue meeting on 5 May 2015 and published by the European Council on 2 June 2015. PSD2 will have to be formally adopted by the Parliament and the Council before it can be published in the Official Journal of the EU. PSD2 will come into force 20 days after it has been published in the Official Journal. It is not clear precisely when PSD2 will be adopted and come into force. However we do know that:

- The European Member States will be obliged to transpose it into their national laws within 2 years of the date when PSD2 comes into force; and
- Payment services providers will be required to comply with the relevant Member State national laws from 2 years after the date when PSD2 comes into force.

The European Parliament / Legislative Observatory file, which records the current position, is available **here**.

NOTES

1. See recitals 3 to 5 of the final compromise text of the second Payment Services Directive (PSD2) (**available here**). **back**
2. Articles 30 to 50. **back**
3. Article 51 to 83 (with the exception of article 73). **back**
4. See article 2. **back**
5. Compare Annex I to PSD1 with Annex I to PSD2. **back**
6. Compare the definitions of "*payment transactions*" in article 3(h) of PSD1 and article 4(5) of PSD2. **back**
7. Articles 31 to 53. **back**
8. Articles 54 to 92. **back**
9. Compare article 2 of PSD1 with article 2 of PSD2. **back**
10. Article 60. **back**