LUXEMBOURG IMPLEMENTS PSD 2

The Luxembourg law dated 20 July 2018 (the "**Law**") implementing the revised Payment Services Directive (EU) 2015/2366 ("**PSD2**") entered into force on 29 July 2018. The Law amends the payment services law of 10 November 2009 on payment services (the "**Payment Services Law**") which had implemented the original Payment Services Directive 2007/64/EC ("**PSD1**").

This briefing outlines the main features of the Law. It is not purported to be a complete discussion of all new features thereof and focuses only on key items.

Key points

- Account information services providers now required to be registered and payment initiation services providers to be licensed
- Narrowing of scope exemptions
- Banks required to grant access to payment account services and payment accounts
- Extension of scope to international transactions
- Increased customer protection and security measures

BACKGROUND

The PSD2 overhauls the existing EU framework for the regulation of payment services under PSD1. It broadens the scope of payment services regulation in the EU and brings third party payment service providers ("**TPPs**") within the scope of EU harmonised regulation for the first time. It also introduces changes to conduct of business requirements aimed at improving consumer protection and competition and changes to security and transparency requirements. It is the result of a number of drivers, including the need to catch up with technology developments, a desire to increase competition in the payments market and facilitate new fintech businesses to provide payment services as well as to react to the increased threat of cyber-attack. The need to strike a balance between these sometimes competing aims of innovation, competition and security has been a common theme throughout the development of PSD2, most notably in relation to the regulation of TPPs and the development of regulatory technical standards that will govern their ability to access payment accounts and related data held with banks and other account providers ("**ASPSPs**").

KEY CHANGES

Key changes introduced by the Law are set out below.

1. Extension of scope

Introduction of AISPs and PISPs as new payment institution types

In addition to the payment services providers already covered by the Payment Services Law, the Law introduces two new types of payment institutions,

Payment Initiation Services Providers ("**PISPs**") and Account Information Services Providers ("**AISPs**"), into the Payment Services Law.

PISPs provide the service of initiating a payment order directly from a customer's bank account, upon request of the customer. The PISPs would typically connect to customers' payment accounts directly online in order to initiate a payment.

AISPs provide the online service of collecting and consolidating in one place information on a customer's sole or multiple bank account(s). Such service would typically enable customers to access the information by online login on the AISP website. Related services can be provided, e.g. statistics showing the customer's budget evolution. As with PISPs, AISPs would typically connect to the customers' payment accounts directly to retrieve the relevant information.

These new payment institutions do not come into possession of client funds at any point, but do have access to client accounts information and, in the case of PISPs, transport the details of the payment instruction.

Key regulatory requirements under the Law for operating as a PISP or AISP are set out in the table below.

PISP	AISP
License as a payment institution required	Application to register in public payment services providers register required
Minimum initial capital: EUR 50,000	No minimum initial capital
Professional civil liability insurance required	Professional civil liability insurance required (but equivalent protection accepted)

Narrowing of exemptions

Most exemptions under the Payment Services Law have been retained by the Law, but some have been narrowed to avoid excessive application. Key changes include:

- **Telecoms:** this exemption is now limited to micro-payments for digital services; high-value payments and payments for purchase of physical goods or services are no longer exempt (*new Art. 3 of the Payment Services Law*).
- **Limited networks:** the Law clarifies that this exemption can only be used for a very limited range of goods/services (or under certain other restrictive conditions) (*new Art. 3 k) of the Payment Services Law*). In addition, payment services providers whose activities exceed EUR 1 million annually will need to notify the CSSF, which will decide whether a license is required (*new Art. 3-1(1) of the Payment Services Law*).
- **Commercial agents:** it is now explicitly set out that agents who negotiate or conclude the sale and purchase of goods or services are only exempt if they act for either the payer or the payee (not both) (*new Art. 3 b) of the Payment Services Law*).

2. Access to payment account services and payment accounts

Access to payment account services

Credit institutions must now provide payment institutions with access to their payment accounts services (i.e. a payment institution must be allowed to open an account if it wishes to do so), and such access must be sufficiently extensive to allow payment institutions to provide payment services in an unhindered and efficient manner (*new Art. 57-1 of the Payment Services Law*).

Access to payments accounts

The Law seeks to ensure that ASPSPs do not undermine the business offerings of TPPs. The Law requires therefore that credit institutions or other ASPSPs provide access to TPPs to online payment accounts.

This access is necessary to allow TPPs to provide their account information or payment initiation services. However, it always requires customer consent, which can never be presumed.

The Law requires a TPP to authenticate itself towards the ASPSP and communicate securely with the ASPSP. However, the Law prohibits ASPPs from requiring TPPs to enter into contracts with them as a condition for allowing such access (although banks may wish to consider incentivising TPPs to enter into contractual arrangements).

In practice, access to payment accounts will in the future be done through an application-programming interface ("**API**"). In order to standardise the use of APIs, the European Banking Authority published *Regulatory Technical Standards on Strong Authentication and Secure Communication* in March 2018, which will apply from September 2019. In the transitional period until then, ASPSPs may need to permit TPP access to payment accounts via screen scraping, unless and until an alternative solution is developed.

3. Extension of scope to international transactions

The Law extends its scope of application to international payments that are partly outside the EU, i.e. to and from a payment services provider located in a third country, as long as the other payment services provider involved in the payment is located in Luxembourg ("one-leg" transactions).

In practice, this means that whenever such an international payment is made involving a Luxembourg-based and a non-EU/EEA based payment services provider, the recast Payment Services Law rules (notably more conduct of business and information requirements) will apply to the Luxembourg side of the transaction.

This applies even if the payment is in a non-EU/EEA Member State currency.

Also, more generally, i.e. also for intra-EU/EEA payments, transactions in non-EU/EEA currencies will now be caught by the provisions of the recast Payment Services Law.

4. Increased customer protection

New conduct of business requirements

The Law reinforces customers' rights. Key examples include:

- **Reduced liability for unauthorised payments:** liability of a payment service user is reduced to a maximum of EUR 50 (compared to EUR 150 previously) for any unauthorised payments due to fraud, abuse or payment incidents (e.g. lost or stolen payment devices) (*new Art. 88 of the Payment Services Law*).
- **Improved refund rights**: customers have an unconditional right of refund for a SEPA direct debit for eight weeks from the date funds are debited from their account (*new Art. 89 (1) of the Payment Services Law*).
- **Responsibility remaining on account managers to reimburse unauthorised payments initiated by PISPs**: in case an unauthorised payment is initiated through the intermediary of a PISP, the ASPSP which manages the account must immediately reimburse the amount of the unauthorised payment (*new Art. 87 (1bis) of the Payment Services Law*).

Security

The Law emphasises customer security and data protection. Payment services providers will be required to update their current procedures to comply with the Law, and will notably have the following obligations:

- **Risk management and reporting to the CSSF**: duties include maintaining an appropriate framework providing for risk mitigation measures and control mechanisms related to the operational and security risks inherent to their payment services activities, reporting on such measures and mechanisms annually to the *Commission de Surveillance du Secteur Financier* ("**CSSF**"), and reporting major operational or security incidents to the CSSF (*new Art. 105-1 and 105-2(1) of the Payment Services Law*).
- **Notification of customers in case of major incidents**: if a security incident might impact customers' financial interests, such customers must be directly notified as well as informed of measures which they may take to mitigate the impact of the incident (*new Art. 105-2(1) of the Payment Services Law*).
- **Strong customer authentication**: application of strong customer authentication procedures is required when the payer accesses its payment account online, initiates an electronic payment operation or executes any action through any means of remote communication that comprises a risk of fraudulent use (*new Art. 105-3 of the Payment Services Law*).

TIMELINE

- **12 January 2016:** PSD2 came into force at EU level
- **10 October 2017:** Luxembourg draft bill implementing PSD2 was introduced
- **29 July 2018:** Luxembourg law transposing PSD2 and amending the law dated 10 November 2009 on payment services entered into force
- **13 January 2019:** end of grandfathering clause for small registered payment institutions and e-money institutions
- **2019 (RTS Application Date):** RTS apply; all AISPs and PISPs must be licensed or registered, and all security measures and strong customer authentication procedures apply, including RTS compliant API use

TRANSITIONAL PROVISIONS

The Law provides for the following main transitional provisions:

- **Transitional period for TPPs:** AISPs and PISPs already active before 12 January 2016 may continue their activities after the entry into force of the Law without authorisation until the date of application of the RTS (the "**RTS Application Date**"), which will be 14 September 2019. Certain security measures linked to third party providers and to strong customer authentication will also only apply on the RTS Application Date.
- **Grandfathering clause:** The Law contains grandfathering provisions, including notably for small registered payment institutions and E-money institutions having received exemption from the CSSF under Art. 48 of the previous Payment Services Law (end of grandfathering period: 13 January 2019).

CLIFFORD
CHANCE

CONTACTS

Christian Kremer
Partner

T +48 50 50 201
E christian.kremer@cliffordchance.com

Steve Jacoby
Partner

T +48 50 50 219
E steve.jacoby@cliffordchance.com

Marc Mehlen
Partner

T +48 50 50 305
E marc.mehlen@cliffordchance.com

Udo Prinz
Counsel

T ++48 50 50 232
E udo.prinz@cliffordchance.com

Amélie Doublet
Associate

T +48 50 50 286
E amelie.doublet@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 10 boulevard G.D. Charlotte, B.P. 1147, L-1011 Luxembourg, Grand-Duché de Luxembourg