POST Finance
LUXEMBOURG

YOUR DAY-TO-DAY SERVICES
PSD2 Information
Payment services

The purpose of this information document is to provide a simple explanation of how "PSD2" works and which benefits it carries. PSD2 is an acronym referring to the second European Directive[1] regarding payment services within the European Union, and more generally to any subsequent legislative or regulatory text arising from it.
This document is intended for information only and you should refer to your Contract, in particular the relevant Accompanying Documents, for details of the rules applicable to you. In particular, the definitions listed in the Glossary are to be read alongside your Contract, and additions have been made to the relevant Accompanying Documents (e.g. Payment Transactions, Online Banking, Cards, etc.).

Vocabulary

English		French	specifically
AISP	account information service provider	prestataire de services d'information sur les comptes	Bank or fintech
ASPSP	account servicing payment service provider	prestataire de services de paiement gestionnaire du compte	Your bank
PISP	payment initiation service provider	prestataire d'initiation de service de paiement	Bank or fintech
PSU	payment service user	utilisateur de services de paiement	You
PSP	payment service provider	prestataire de services de paiement	Bank or fintech
SCA	strong customer authentication	authentification forte du client	Secure means

Persons concerned
PSD2 applies to what we call PSPs, which are mainly banks providing payment services to their customers (e.g. POST Finance to you). However, other service providers are also affected by the requirements of PSD2, such as PISPs, AISPs and even electronic money and payment institutions. The applicability of PSD2 depends solely on the provision of payment service(s) and not on the nature of other activities, the type of customers served or the size of the institution.

Content
Information: PSD2 requires PSPs to be more transparent about the information that is communicated to PSUs concerning fees, transaction turnaround times, the use of payment instruments, complaints, your rights to refunds, etc.

Transactions: thanks to the entry into force of the PSD2, all PSPs in Europe must, in principle, execute payments that are made exclusively within the European Union and in a European currency within one business day (from the date of receipt of the Payment Order). As a result, turnaround times and the availability of funds are generally reduced.

Responsibility: PSD2 increases the accountability of PSPs for the correct execution of payment transactions.

Refunds: payment transaction refund conditions have improved for PSUs.

Incidents: any incident considered to be major will have to be reported directly to the competent authority (for Luxembourg, this is the CSSF[2]) and the relevant PSP will notify the PSU if the incident could affect its financial interests.

Fraud: By imposing new obligations regarding risk, security, oversight and the reporting of statistics associated with fraud, PSD2 aims to help PSPs to better protect you against fraud. To limit them, PSD2 also requires ASPSP to implement Strong Authentication for their PSUs for all remote access to account information or payment initiation.

Strong authentication
Strong authentication is a means of identifying PSUs based on at least two of the following three authentication elements:
- possession (e.g. an electronic key/token);
- knowledge (e.g. a password);
- inherence (e.g. a fingerprint, any biometric element).

These elements must be independent of one another, so that if one of them is compromised, this will not affect the reliability of the others. The combination of two of these elements leads to the generation of an authentication code that is accepted only once.

[1] EU Directive 2015/2366 of 25 November 2015
[2] Commission de Surveillance du Secteur Financier

When strong authentication is used for payment initiation purposes, the authentication code is dynamically linked to the amount and the payee.
POST Finance provides strong authentication thanks to the LuxTrust solution.

Strong authentication is required when a PSU (or a PISP or AISP that it has mandated):
- accesses its online payment account;
- initiates an electronic payment transaction; or
- executes an action, via remote communication, which may involve a risk of fraud with regard to payment, or some other fraudulent use.

Under certain conditions, some access or initiations of payment transactions may nevertheless be exempted from strong authentication, for example:
- access to the balance of one or more payment accounts and to a transaction history that is less than 90 days old;
- initiation of a payment to a trusted payee;
- initiation of a low value payment;
- initiation of a payment to another of the payer's accounts;
- initiation of a payment considered to be low risk.

New actors

PSD2 mainly introduces two new types of actors (PISPs and AISPs), regulated and supervised (by the CSSF or by another competent authority within the EU), on the payments market, which can initiate payments from or access information about PSU accounts held with another PSP (which is then designated as an ASPSP):
These are service providers who, with the explicit and prior consent of the PSU:
- (**PISPs**) initiate payment transactions from a payment account held with another entity (e.g. a bank); or
- (**AISPs**) collect information on one or more payment accounts held with one or more other entities (e.g. account aggregators).

Revocation of a payment order

PSUs cannot revoke a payment order after it has been received by a PSP. When the payment order is initiated by a PISP or via the payee, a PSU cannot revoke the payment order:
- once they have agreed to the PISP initiating the payment transaction, or
- after forwarding the payment order to the payee of said payment order, or
- once they have given their consent for the execution of a payment order directly to the payee of said order.

Liability in the event of unauthorised Payment Transactions

If a payment transaction has been initiated directly by the PSU but cannot be considered to have been authorised by the PSU, including when it has used a PISP, the PSP/ASPSP of the PSU will reimburse the latter with the amount of the payment transaction immediately upon becoming aware or having been informed of this, unless it has good reason to suspect fraud and communicates those reasons to the competent authority.
The PSU may be required to bear any losses associated with unauthorised payment transactions resulting from the use of a lost, stolen or diverted payment instrument up to a limit of 50 EUR unless such loss or theft cannot be attributed to it or unless the transaction initiated constitutes a breach of the legal obligation of the PSP/ASPSP to implement strong authentication. In any case, the PSU will be required to bear all losses relating to the payment transaction in the event of fraud on its part.
If the PISP is found to be responsible for the unauthorised payment transaction, it will indemnify the PSP/ASPSP in accordance with the Law, since this process does not involve the PSU and is handled exclusively between the PISP and the ASPSP.

Liability in the event of the non-execution, incorrect execution or late execution of Payment Transactions

If a payment transaction has not been executed or has been executed incorrectly (including late), and the PSU initiated the payment order, including cases in which it has used a PISP, the PSP/ASPSP of the PSU will reimburse the amount of the non-executed or incorrectly executed payment transaction, provided that:
- the non-execution or incorrect execution is not due to the provision of an incorrect unique identifier by the PSU;
- the non-execution or incorrect execution is not due to a case of force majeure; and
- the PSU has notified the PSP/ASPSP of the non-execution or incorrect execution in accordance with the procedures put in place by the PSP/ASPSP.

If the PSP/ASPSP of the PSU can prove that the payee of the payment transaction has received the funds, however, it is the payee's PSP that is liable.
If the PISP is found to be responsible for the non-executed or poorly executed payment transaction, it will indemnify the PSP/ASPSP in accordance with the Law. This process does not involve the PSU and is handled exclusively between the PISP and the ASPSP.

Impacts on your Services

Payment initiation and account information: new services?

No. You already have access to these payment initiation and account information services, since you can access your POST Finance account information and initiate payments via POST Finance Online Banking.
The new aspect arises from the fact that POST Finance and regulated entities can now also offer you these payment initiation and information services in connection with your Account held with POST Finance or with other ASPSPs/TPPs using LUXHUB services. However, you will need to activate your Online Banking access to benefit from these services and POST Finance may not be held responsible if this is not the case.
You can use the payment initiation and account information services provided by PISP or AISP duly authorised for this purpose in Luxembourg or in another EU Member State in connection with your POST Finance Account.
You are entitled to the same level of services whether you go directly via POST Finance Online Banking or via AISPs/PISPs.

And your accounts held elsewhere?
POST Finance can offer you a new feature for aggregating external payment accounts and initiating payments from these accounts. It then acts as an AISP and/or PISP itself. You will then benefit from two new services: the Payment Initiation Service and the Account Information Service for your accounts with other financial institutions. Therefore, by logging into your POST Finance Online Banking app and having given your consent, you will be able to initiate payments from your payment accounts held with another financial institution and consult information on your POST Finance Accounts and those with said financial institution. POST Finance may decide to withdraw a banking institution from its list or terminate the account aggregation service without having to provide its reasons for doing so. In order to improve the operation of the account aggregation service and to maintain it, POST Finance may also suspend access for a specified period and without notice.
You can change the settings at any time (show or hide the accounts of your choice, delete the added financial institutions, or disable the account aggregation service). The list of financial institutions concerned will be available in your POST Finance Online Banking application.