PaymentsCompliance

1. Strong customer authentication: key provisions of PSD2

Article 98 of Directive 2015/2366, also known as the revised Payment Services Directive (PSD2) mandates the European Banking Authority (EBA), in close cooperation with the European Central Bank (ECB), to develop "draft regulatory technical standards", specifying:

- Requirements for strong customer authentication.
- Exemptions from the application of strong customer authentication.
- Requirements with which security measures have to comply, to protect the confidentiality and the integrity of the payment service users' personalised security credentials.
- Requirements for common and secure open standards of communication for the purpose of identification, authentication, notification and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.

Pursuant to Article 97(1) of PSD2, payment service providers (PSPs) should apply strong customer authentication when the payer:

- Accesses their payment account online.
- Initiates an electronic payment transaction. For electronic remote payment transactions, PSPs should apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.
- Carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

In accordance with Article 98(3) of PSD2, the EBA must observe the following criteria when establishing exceptions from strong customer authentication measures:

- The level of risk involved in the service provided.
- The amount, the recurrence of the transaction, or both.
- The payment channel used for the execution of the transaction.