Payment services in the internal market

2013/0264(COD) - 03/04/2014 - Text adopted by Parliament, partial vote at 1st reading/single reading

The European Parliament adopted **amendments** to the proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC.

The matter was referred back for further examination to the committee responsible. The vote was postponed until a subsequent plenary session.

The main amendments adopted in plenary were the following:

Safe electronic payments: given the development of the digital economy, Parliament stated that it was in favour of establishing an **integrated single market for safe electronic payments** was crucial in order to support the growth of the Union economy and to ensure that consumers, merchants and companies enjoy choice and transparency of payment services to benefit from the full benefits of the internal market.

Consumer information: Parliament called for charges for information to be reasonable and in line with the payment service provider's actual costs.

Consumers who **switch their payment account**, upon request can receive the transactions carried out on the former payment account recorded on a durable medium from the transferring payment service provider for a reasonable fee. The burden of proof should lie with the payment service provider to prove that it has complied with the information requirements.

The amended text stipulates that for payment initiation services, the third party payment service provider should, prior to initiation, **provide the payer with the following clear and comprehensive information:**

- the contact information and registration number of the third-party payment service provider, and the name of the supervisory authority responsible;
- where applicable, the maximum time-limit for the payment initiation procedure;
- all possible charges payable by the payment service user to the third-party payment service provider and, where applicable, the breakdown of the amounts of any charges;
- where applicable, the actual or reference exchange rate to be applied.

These provisions are without prejudice to the data protection obligations applicable to the third-party payment service provider and the payee.

Access of third-party payment service providers and third-party payment instrument issuers to payment account details: the amended text stated that Member States should ensure that a payer who held a payment account that could be accessed via online banking, has the right to make use of an authorised third party payment service provider, to obtain payment services enabling access to payment accounts. A payer should have the right to make use of an authorised third-party payment instrument issuer to obtain payment instrument enabling payment transactions.

Furthermore, payees who offered to payers the option of making use of third party payment service providers or third-party payment instrument issuers should **unambiguously provide to payers information** about such third party payment service provider(s), including their registration number and the name of their responsible supervisory authority.

Notification of unauthorised or incorrectly executed payment transactions: the payment service user should **report to its account servicing payment service provider any incident** known to them that affected the former in the context of its use of a third-party payment service provider or third-party payment instrument issuer.

If the payment service user initiated the payment transaction through a third party payment service provider, the burden shall be on the latter to prove that the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiencies.

Liability: in the case of an unauthorised payment transaction, the payer's payment service provider must refund the amount to the payer **within 24 hours of having noted or having been notified about the transaction**.

If the third party payment service provider cannot demonstrate that it is not liable for the unauthorised payment transaction, it should, **within one business day**, compensate the account servicing payment service provider for reasonable costs incurred as a result of the refund to the payer, including the amount of the unauthorised payment transaction.

By way of derogation, **the payer may be obliged to bear the losses, up to a maximum of EUR 50** or the equivalent in another national currency, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument. This should not apply if the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment.

The payer **should not bear any financial consequences resulting from use of a lost, stolen or misappropriated payment instrument** if the resulting unauthorised payment was made possible by a method or a security breach, that had already been known and documented and the payment service provider failed to enhance security schemes to effectively block further attacks of that kind, except where the payer himself has acted fraudulently.

Data protection: processing of personal data by payment systems and payment service providers **should only be permitted when this is necessary** to safeguard the prevention, investigation and detection of payment fraud.

Parliament called for the principles of data protection privacy by design/privacy by default to be embedded in all data processing systems developed and used within the framework of this Directive.

Management of operational risks: payment service providers should **establish a framework with appropriate mitigation measures and control mechanisms** to manage the operational risks, including security risks, relating to the payment services they provide. As part of that framework payment service providers shall establish and maintain effective incident management procedures, including the detection and classification of major incidents.

Common and secure open standards of communication: it is proposed that EBA should, in close cooperation with the ECB develop draft regulatory technical standards in the form of common and secure open standards of communication. The common and secure open standards of communication should in particular, specify **how third-party payment service providers are to authenticate themselves** towards account servicing payment service providers and how account servicing payment providers are to notify and inform third-party payment service providers.

List of payment services providers: Parliament called for the **EBA to make available** on its website a list of all the authorised payment services providers within the Union.

That list should refer to all authorised payment services providers whose registration has been revoked and the reasons for this.

Electronic leaflet: Members suggested that within two years of the entry into force of the Directive, the Commission should produce a consumer friendly electronic leaflet listing, in a **clear and easily comprehensible manner, the rights and obligations of consumers** laid down in the Directive and in related Union law on payment services.

This information should be made available on the websites of the Commission, the European Supervisory Authority (European Banking Authority - 'EBA'), and national banking regulators.