PAYMENT SERVICES: PSD II

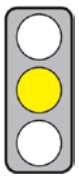
cep**PolicyBrief** No. 2014-11

Centrum für Europäische Politik

KEY ISSUES

Objective of the Directive: The Commission wants to promote the European payments market and encourage transparency, security and innovation in relation to payments.

Affected parties: Payment service providers, payment service users, banks, merchants.



Pro: (1) The inclusion of third-party payment service providers within the scope of application clarifies their responsibilities, duties and liability.

(2) The rule that Member States can no longer prohibit charges for the use of payment instruments facilitates cross-border trade.

Contra: (1) The rules on "limited networks" and "digital payment transactions" create incentives for regulatory arbitrage and distort competition.

(2) The obligation to increase customer authentication requirements for electronic payments should be rejected.

(3) The ban on extra charges to end-customers for payment by credit and debit cards restricts competition without just cause.

CONTENT

Title

Proposal COM(2013) 547 of 24 July 2013 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

Brief Summary

Note: In the absence of any indication to the contrary, article numbers refer to the 2nd Payment Services Directive (PSD II)

- **Context, definitions and objectives**
  - This Payment Services Directive (PSD II) replaces the existing PSD I (2007/64/EC).
  - At the same time, the Commission is proposing the introduction of an upper limit for interchange fees for card-based payments [COM (2013) 550].
  - The Directive covers, inter alia, the following payment services (Art. 4 (3), Annex 1)
    - services enabling cash to be withdrawn from or placed on a payment account,
    - services enabling the execution of payments via credit or debit cards,
    - services enabling the execution of direct debits and transfers of funds.
  - Payment services are carried out by payment service providers. Payment service providers are inter alia (Art. 1)
    - companies that specialise in providing payment services ("payment institutions"),
    - companies that handle on-line payments ("electronic money institutions"), and
    - banks.
  - Payment instruments are devices that can be used to initiate a payment, e.g. cash, cheques, credit cards.
  - The Commission wants (Explanatory Memorandum, pages 10-12)
    - to extend the scope of PSD I,
    - to regulate surcharges imposed by merchants for the use of certain payment instruments,
    - to revise the existing rules on refunds in the case of direct debits and the rules on liability in the case of unauthorised payments and
    - to introduce stricter security requirements for payment service providers.
- **Basic provisions of the Payment Services Directives PSD I and PSD II**
  - Payment service providers, that provide payment services covered by the Directive,
    - require an authorisation (Art. 10) and must be entered in a national register (Art. 13),
    - must comply with own funds requirements (Art. 7 and 8),
    - are subject to transparency requirements relating, for example, to charging conditions (Art. 31-53) and
    - must comply with obligations relating to the provision of payment services, e.g. the cancellation of payments where necessary (Art. 54-92).
  - Payment service providers can provide payment services in all Member States ("passporting") (Art. 18).
- **Extension of scope**
  - **Third-party payment service providers**
    - In future, the Directive will also apply to "third-party payment service providers". These are payment service providers that do not provide the user with a payment account but allow him access to his accounts with other payment service providers via a "software bridge". (Art. 3 (j), Art. 4 (11))

Authors: Philipp Eckhardt and Anne-Kathrin Baran | eckhardt@cep.eu
cep | Kaiser-Joseph-Strasse 266 | 79098 Freiburg | Germany | Telephone +49 (0)761 38693-105 | www.cep.eu

- Software bridges are used in order to (Art. 4 No. 32 and 33)
  - initiate payments - e.g. in on-line banking - from the holder's own accounts ("payment initiation services"),
  - to obtain consolidated information about the user's own accounts ("account information services").
- Third-party payment service providers (Art. 58 (1) and (2))
  - must ensure that unauthorised parties do not gain access to the user's "security features",
  - must clearly authenticate themselves towards the account servicing payment service provider and
  - must not store any "sensitive" payment data or "personalised security credentials" of the user.
- When a payment is initiated, the account servicing payment service provider must "immediately" notify the third-party payment service provider of the receipt of the payment order and indicate whether there are sufficient funds in the account (Art. 58 (3)).
- Users have the right to gain access to their payment accounts via third-party payment service providers (Art. 58 (1)).

– **Exceptions regarding the acquisition of "a limited range" of products and for "limited networks"**
- Until now, the Directive did not apply to payment services based on payment instruments – mainly certain cards – and used for the acquisition of "a limited range" of products from the issuer of the payment instrument or in a "limited network" of merchants with whom the issuer has an agreement (Art. 3 (k) PSD I). This includes petrol cards or store cards.
- In future these exceptions will only apply where the payment instruments (Art. 3 (k))
  - are "specific",
  - address "precise needs" and
  - can be used "only in a limited way".

  The terms are not defined in more detail so definition is left up to the discretion of the Member States.
- Use of the payment instrument in a "limited network" by merchants is only permitted if the responsible authority "recognises" the said network. The recognition obligation does not apply if monthly average payments do not exceed one million euro. (Art. 30 (2))

– **Exceptions for digital payment transactions in conjunction with "digital content"**
- Until now, the Directive did not apply to payment transactions allowing the purchase of products by way of electronic devices - e.g. smart phones - if the acquired goods or services were delivered on a device "for use by way of the same". These operators of telecommunications infrastructure required for purchase are, however, not deemed to be payment service providers, if they do not act only as "intermediaries" between the payment service user and the supplier of the goods and services (Art. 3 (l) PSD I)
- In future, the Directive will not apply to payment transactions allowing the purchase of "digital content" – e.g. apps, ring tones. Operators of the telecommunications infrastructure necessary to make the purchase shall not be deemed to be payment service providers if (Art. 3 (l)
  - the payment transaction is carried out as “ancillary service” to communications services and
  - a user's single purchase amount does not exceed € 50 or all purchases by a user do not exceed € 200 in one month.

► **Charges for the use of payment instruments**
– Until now, Member States could ban charges for the use of certain payment instruments (Art. 52 (3) PSD 1). In future, this right will not apply (Art. 55 (3)).
– As before, merchants may impose a charge on payers for the use of a specific payment instrument or grant them a reduction (Art. 52 (3) PSD I, Art. 55 (3). In future, they will also be able to "otherwise steer" payers towards a payment instrument (Art. 55 (3)).
– In future, merchants will only be able to impose a charge for the use of a specific payment instrument amounting to the costs which they incur (Art. 55 (3)).
– In future, merchants will no longer be able to charge specifically for the use of debit and credit cards by their end-customers (Art. 55 (4)).

► **Rules on refunds and liability**
– **New rules on refunds of direct debits**
- Until now, in the case of direct debits, payers have only been entitled to a refund where (Art. 62 (1) PSD I)
  - on authorisation of the payment the precise amount was not specified,
  - the payment amount was unusually high or
  - a contract between the payer and payment service provider provides for a refund for other reasons.
- In future, in the case of direct debits, payers will have an "unconditional" right for refund within eight weeks. This does not apply, however, if a payee has already fulfilled its contractual obligations and the payer has received the service or "consumed" the goods. At the request of the payment service provider, payees must prove that they have fulfilled their contractual obligations. (Art. 67 sub-paragraph. 3 and 4)

– **Liability for unauthorised or incorrect payments**
- Until now, payment service providers have been able to require payers to share, up to a maximum of € 150, in the loss arising as a result of payments with a stolen, lost or misappropriated payment instrument (Art. 61 (1) PSD I). In future the amount will drop to € 50 (Art. 66 (1), sub-paragraph 2).

- Where a payer denies having "authorised" a payment, it is still the case that payment service providers must prove that they have checked the identity of the payer and that the payment has been properly processed and entered into the accounts. The same applies where the payer claims that the payment was "not properly" carried out (Art. 59 (1) PSD I). In future, this will also apply to third-party payment service providers (Art. 64).
- As before, payment service providers must reverse unauthorised payment entries on the payer's account (Art. 60 PSD I). In future, this will also apply where a third-party payment service provider is involved. In this case, the account servicing payment service provider may claim compensation from the third-party payment service provider if the latter is at fault. (Art. 65)

► **Security measures, reporting obligations and strong customer authentication**

– In future, the Directive on Network and Information Security [NIS-Directive, COM (2013) 48, see cep**PolicyBrief**] (Art. 85 (1)) will apply to payment service providers.

– Thus they must (Art. 14 and 15 NIS Directive)
  - take security measures in order to "manage" security risks and incidents and
  - report, to the competent authority, security incidents, which have a "significant" impact on the security of its core services.

– In future, payment service providers - including third-party payment service providers - will have to implement "strong customer authentication" when they initiate an "electronic payment transaction" (Art. 87 (1)).

– The European Banking Authority will issue guidelines on the authentication procedure. It can exempt certain payment services from the obligation to provide strong authentication. (Art. 87 (3))

Statement on Subsidiarity by the Commission

According to the Commission, an integrated payments market can only be achieved by way of action at EU level.

Policy Context

The Payment Services Directive (2007/64/EC) is the relevant regulatory framework for payment services. Regulation [(EC) No. 924/2009] regulates cross-border payment transactions (see cep**PolicyBrief**). The SEPA Regulation [(EU) No. 260/2012] provides rules on transfers and direct debits in euro. The Electronic Money Directive (2009/110/EC; see cep**PolicyBrief**) regulates the issue and exchange of e-money and lays down supervisory regulations for e-money institutions. The Wire Transfer Regulation [(EC) No. 1781/2006] requires payment service providers to transfer details about the payer. A new Regulation [COM (2013) 44, see cep**PolicyBrief**] is planned. The Federal Cartel Authority examines whether the banks' terms and conditions are in breach of competition law (Art. 101 TFEU, Section 1 GWB) because they only permit on-line banking via certain internet sites.

Legislative Procedure

24 July 2013 Adoption by the Commission
Open Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Leading Directorate General	DG Internal Market
Leading Committee of the EP:	Economic and Monetary Affairs; Rapporteur Diogo Feio (EVP-Group, PT)
Leading Federal Ministry:	Ministry of Finance
Leading Committee of the BT:	Finance
Decision-making mode in the Council:	Qualified majority (Adoption by a majority of the Member States and with 260 of 352 votes; Germany: 29 votes)

Formalities:

Legislative competence:	Art. 114 TFEU
Form of legislative competence:	Shared competence (Art. 4 (2) TFEU) Legislative procedure:
Procedure:	Art. 294 TFEU (Ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

The inclusion of third-party payment service providers within the scope of the Directive **clarifies their responsibilities, duties and liability.** In particular, the duty to protect the payer's security features from access by third parties and the ban on storing sensitive payment data or personalised security data also contribute to this. The right of the payer to gain access to his accounts via third-party payment service providers is equivalent

to a duty upon banks to allow third-party payment service providers access to the bank's own payment system. **A bank should only have to grant access to third-party payment service providers where the bank has an unassailable position on the consumer market.** Competition authorities - not the legislator - should decide on this in the individual case.

More account should be taken of the differences between the activities of third-party and conventional payment service providers: Third-party payment service providers are purely IT service providers and never come into direct contact with the transferred monies. This must be taken into account - for example in own funds requirements.

The approach to the rules on exceptions to the Directive – for the acquisition of "a limited selection" of goods, **for "limited networks" and for "digital payment transactions"** is unconvincing. In future, national legislators and regulatory authorities will still be able to decide when, for example, a "limited network" exists or when a digital payment transaction constitutes an "ancillary service". The resulting discretionary latitude **creates incentives for regulatory arbitrage and distorts competition**.

The rule that Member States can no longer prohibit charges for the use of payment instruments **facilitates cross-border trade because** sellers can apply a standard pricing policy in all 28 Member States. In addition, the new rule **is efficient**: it allows merchants to charge accordingly for the varying costs incurred for the different payment instruments. This encourages customers to use the most efficient and cost-effective payment instrument, and thereby **strengthens competition** on the payment instrument market **and puts an end to the unjustifiable cross-subsidisation of payment instruments.** Apart from where the individual merchant had an unassailable market position, the obligation to base charges for the use of payment instruments on the cost of use is ill-founded because excessive charges are not enforceable where there is competition.

The ban on extra charges to end-customers specifically **for payment by credit and debit cards restricts competition** also **without just cause.** The ban is all the more confusing because the Commission does not want to ban but only restrict interchange fees, which are similar to wholesale prices [COM (2013) 550].

The Commission is attempting to combat misuse by way of the restrictions on the right to reimbursement in the case of direct debits. The cost of this, however, is very high because the payment service provider is forced to deal with legal matters arising in a different sector. Any conflicts should continue to be settled between the payee and the payer - i.e. within the contractual relationship where the dispute exists.

The inclusion of the payment service provider within the provisions on network and information security ("NIS Directive", COM (2013) 48, see cep**PolicyBrief**) **is justified.** Service providers have an interest in protecting their infrastructure against failures and intrusions because such incidents involve loss of revenue and damage to reputation. **Intrusions are not always apparent** to the public, however, **so payment service providers are often not held liable.** The fact that payment service providers are obliged to take security measures is therefore appropriate because the liability principle is not sufficiently effective.

The obligation to use "strong" customer authentication for electronic payment transactions should be rejected. Although it increases the security of payment transactions and strengthens the user's confidence because it makes fraudulent acts more difficult, it also involves costs. Payment service providers and end-users should be able to decide freely between a "simple" and a "strong" customer authentication. The requirement for this is the service provider's obligation to provide the customer with transparent information in this regard.

Legal Assessment

Legislative Competency

The proposal is correctly based on the internal market competence (Art. 114 TFEU).

Proportionality

Unproblematic.

Compatibility with EU Law in other Respects

By only prohibiting payees from imposing charges where interbank charges have been established for the respective payment instrument, the Directive breaches the principle of equality (Art. 20 EU Charter of Fundamental Rights) because there is no justification for this unequal treatment.

Impact on German Law

In Germany, the Payment Services Supervisory Act (ZAG) will have to be amended.

Conclusion

The inclusion of third-party payment service providers clarifies their responsibilities, duties and liability. A bank should only have to grant access to third-party payment service providers where the bank has an unassailable market position on the consumer market. The rules on "limited networks" and "digital payment transactions" create incentives for regulatory arbitrage and distort competition. The fact that Member States can no longer prohibit charges for the use of payment instruments facilitates cross-border trade. The ban on extra charges to end-customers for payment by credit and debit cards restricts competition without just cause. The inclusion of payment service providers within the provisions on network and information security is justified. The obligation to use "strong" customer authentication for electronic payment transactions should be rejected.