

III

(Preparatory acts)

EUROPEAN CENTRAL BANK

OPINION OF THE EUROPEAN CENTRAL BANK

of 5 February 2014

on a 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

(CON/2014/9)

(2014/C 224/01)

Introduction and legal basis

On 31 October 2013, the European Central Bank (ECB) received a request from the Council for an opinion on a proposal for a directive 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⁽¹⁾ (hereinafter the 'proposed directive').

The ECB's competence to deliver an opinion is based on Articles 127(4) and 282(5) of the Treaty on the Functioning of the European Union since the proposed directive contains provisions affecting the tasks of the European System of Central Banks (ESCB) to promote the smooth operation of payment systems and to contribute to the smooth conduct of policies relating to the stability of the financial system, as referred to in the fourth indent of Article 127(2) and Article 127(5) of the Treaty. In accordance with the first sentence of Article 17.5 of the Rules of Procedure of the European Central Bank, the Governing Council has adopted this opinion.

General observations

1. The proposed directive, which incorporates and repeals Directive 2007/64/EC⁽²⁾ ('Payment Services Directive' or 'PSD'), aims to help further develop a Union-wide market for electronic payments, thereby enabling consumers and market participants to fully benefit from the internal market, also taking into account the rapidly developing retail payment market (the introduction of new payment solutions via smart phones, e-commerce, etc.). These proposals follow an extensive review by the Commission of the current payment services environment. In January 2012, the Commission published and publicly consulted its Green Paper towards an integrated European market for card, internet and mobile payments⁽³⁾, to which the ECB also responded⁽⁴⁾. Both the responses to the consultation on the Green Paper and the Commission's own studies and review of the PSD reveal that recent innovations in the market and in technology for retail payment services pose new challenges for regulators, which the proposals aim to address.
2. The proposed directive introduces numerous amendments to the current PSD regime, including extending coverage as regards the geographical scope and currency of payment transactions. It redefines and amends a number of the current exemptions from the PSD, to make them tighter and more difficult to exploit, and deletes others that are no longer required. For example, it amends the exemption for 'commercial agents' so that it will only apply to commercial agents that act on behalf of either the payer or the payee. It also redefines the current digital content or 'telecom' exemption with a more restricted focus and removes the exemption from the PSD of ATM services offered by independent ATM

⁽¹⁾ COM(2013) 547/3.

⁽²⁾ Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (OJ L 319, 5.12.2007, p. 1).

⁽³⁾ COM(2011) 941 final.

⁽⁴⁾ See Eurosystem response to the European Commission Green Paper 'Towards an integrated European market for card, internet and mobile payments' of March 2012, available on the ECB's website at www.ecb.europa.eu.

deployers. Most significantly, it extends the PSD regime to cover new services and their providers, i.e. 'third party payment service providers' ("TPPs") whose business activity is providing services based on access to payment accounts, such as payment initiation or account information, but who do not usually hold client funds⁽⁵⁾. It also prohibits the practice of merchants imposing surcharges for interchange fee-regulated cards, in view of the capping of interchange fees under the proposed regulation on interchange fees for card-based transactions⁽⁶⁾. Finally, it also amends numerous important components of the current regime- such as for example the safeguarding requirements, waiver conditions, and payment service provider (PSP) and payer liability for unauthorised payment transactions - with a view to further harmonising these provisions, develop a more level playing field and improve legal certainty⁽⁷⁾. The proposed directive is generally intended to give consumers increased protection against fraud, possible abuses and other incidents related to the security of payment services. It contains several provisions requiring the European Banking Authority (EBA) to contribute to the consistent and coherent functioning of supervision pursuant to Regulation (EU) 1093/2010 of the European Parliament and of the Council⁽⁸⁾.

3. The ECB strongly supports the objectives and the content of the proposed directive. In particular, it supports the proposal to extend the current list of payment services to include payment initiation services and account information services as a means to support innovation and competition in retail payments. Supervisors and overseers have extensively discussed the issue of third party access to payment accounts in the context of the European Forum on the Security of Retail Payments (hereinafter the 'SecuRe Pay Forum'). The core elements of these discussions are reflected in the ECB's drafting proposals.

4. The ECB also welcomes the fact that: (a) harmonisation and improvement of operational and security requirements for payment service providers has been proposed; (b) the competent authorities' enforcement powers are to be strengthened; and (c) certain provisions of the PSD, whose application Member States have had considerable discretion over up to now, are to be tightened. This element of discretion has led to considerable divergence in the application of the rules across the Union and consequent fragmentation of the retail payments market⁽⁹⁾. The ECB previously made its views known in its response to the Green Paper⁽¹⁰⁾ and also in other forums such as the SecuRe Pay Forum. The ECB is pleased that many of the recommendations made in that response and also by the SecuRe Pay Forum have been covered in the proposed directive. Nonetheless, the ECB has a number of specific comments.

Specific observations

1. *Defined terms*

The defined terms of the proposed directive⁽¹¹⁾ are largely unchanged from those of the PSD, but they could be further improved. In particular, the definitions 'issuing of payment instruments' and 'acquiring of payment transactions' should be added to the proposed directive⁽¹²⁾. This would give Annex I to the proposed directive greater clarity. The definitions 'payment initiation service'⁽¹³⁾ and 'account information service'⁽¹⁴⁾ could also be improved by further amendment, and definitions of 'credit transfer', 'cross-border payments' and 'national payments' should be included for the sake of completeness.

⁽⁵⁾ See Point (7) of Annex I to the proposed directive.

⁽⁶⁾ Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions (COM(2013) 550/3); 2013/0265.

⁽⁷⁾ Further provisions clarify the rules on access to payment systems and the right of refund, and also address the security aspects and aspects of authentication in line with the Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union (COM(2013) 48 final) (hereinafter the 'Network and Information Safety (NIS) Directive');. For the proposed NIS Directive see further para. 2.12 below.

⁽⁸⁾ Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).

⁽⁹⁾ See, for example, Article 66 of the proposed directive on the rules on PSP and payer liability in case of unauthorised card transactions.

⁽¹⁰⁾ See footnote 4.

⁽¹¹⁾ See Article 4 of the proposed directive.

⁽¹²⁾ See drafting amendment 12 in the Annex.

⁽¹³⁾ See Article 4(32) of the proposed directive.

⁽¹⁴⁾ See Article 4(33) of the proposed directive.

2. **Other provisions**

- 2.1. As regards the scope of application⁽¹⁵⁾, the proposed directive provides that, where only one of the payment service providers to a payments transaction is located within the Union, the provisions with regard to the credit value date⁽¹⁶⁾ and on transparency of conditions and information requirements for payment services shall apply to those parts of the transaction that are carried out in the Union⁽¹⁷⁾. To the extent possible, Title IV, which covers rights and obligations in relation to the provision and use of payment services, should also apply in such cases and should apply equally in respect of all currencies.
- 2.2. The proposed directive does not retain the possibility contained in the current PSD that authorises Member States or competent authorities to extend safeguarding requirements applicable to payment institutions engaged in business activities other than payments to payment institutions only involved in the provision of payment services⁽¹⁸⁾. The ECB would propose that payment institutions should have an obligation to provide appropriate protection in the form of the safeguarding requirements for a payment service user's funds, regardless of whether they are engaged in other business activities than payment services or not.
- 2.3. For reasons of efficiency, the ECB would welcome one single authority, which would be responsible for ensuring compliance with the directive, but is aware, however, that this might prove difficult in practice due to diverging national arrangements.
- 2.4. Furthermore, the ECB suggests that Europol be added as an additional authority with which the competent authorities for supervising payment services may exchange information⁽¹⁹⁾, in view of Europol's expertise in the area of international crime and terrorism, including combatting euro counterfeiting and other misuse of payment instruments and services for the purposes of financial crime.
- 2.5. Considering that account servicing payment service providers shall, for services under point 7 in Annex I to the proposed directive, be mandated to allow access to payment accounts, and also taking into consideration that TPPs' services are usually provided over the internet and therefore not limited to one single Member State, the ECB suggests, for security reasons, that TPPs should not be the cause for any waiver under Article 27.
- 2.6. Payment systems designated under Directive 2009/44/EC⁽²⁰⁾ (hereinafter the 'Settlement Finality Directive') are excluded from the rule in Article 29(1) of the proposed directive, which states that access to payment systems should be objective and non-discriminatory. However, the last paragraph of Article 29(2) of the proposed directive states that, if a designated payment system allows indirect participation, such participation should also be provided to other authorised or registered payment service providers in accordance with Article 29(1). The definition of 'indirect participant' in Article 2(g) of the Settlement Finality Directive does not currently cover payment institutions and, in order to ensure consistency and legal certainty, the ECB suggests amending the definition of 'indirect participant' in the Settlement Finality Directive to also cover payment service providers.
- 2.7. In order to combine security requirements and customer protection with the idea of open access to payment account services, the ECB suggests that customers are appropriately authenticated by relying on a strong customer authentication system. TPPs could ensure this through either redirecting the payer in a secure manner to their account servicing payment service provider or issuing their own personalised security features. Both options should form part of a standardised European interface for payment account access. This interface should be based on an open European standard and allow any TPP to access payment accounts at any PSP throughout the Union. The standard could be defined by EBA in

⁽¹⁵⁾ See Article 2 of the proposed directive.

⁽¹⁶⁾ See Article 78 of the proposed directive.

⁽¹⁷⁾ See Title III of the proposed directive.

⁽¹⁸⁾ See Article 9 of the PSD.

⁽¹⁹⁾ See Article 25 of the proposed directive.

⁽²⁰⁾ Directive 2009/44/EC of the European Parliament and of the Council of 6 May 2009 amending Directive 98/26/EC on settlement finality in payment and securities settlement systems and Directive 2002/47/EC on financial collateral arrangements as regards linked systems and credit claims (OJ L 146, 10.6.2009, p. 37).

close cooperation with the ECB and include technical and functional specifications, as well as related procedures. Furthermore, third party payment service providers should: (a) protect the personalised security features of payment service users they issue themselves; (b) authenticate themselves in an unequivocal manner vis-à-vis the account servicing payment service provider(s); (c) refrain from storing data obtained when accessing payment accounts, apart from information that identifies payments they initiate, such as reference number, payer's and payee's IBAN as well as the transaction amount; and (d) refrain from using data for any purposes other than those explicitly permitted by the payment service user⁽²¹⁾. Contracts between the account servicing payment service providers and the TPPs are one possible option for clarifying a number of these aspects. From an efficiency perspective, and in order not to create an undue barrier to competition, the main aspects (including a liability regime) should be clarified in the proposed directive. Further business rules, including technical and operational arrangements, e.g. authentication, protection of sensitive data, identification and traceability of payment orders could be defined through the creation of a payment scheme, to which all relevant actors could adhere and which would avoid the need to seek agreement on individual contracts.

- 2.8. Concerning the provisions on framework contracts and consumer protection the ECB is of the view that consumers, as payment account holders in relation to payment initiation services, should have a level of protection comparable to that provided to debtors under Regulation (EU) No 260/2012 of the European Parliament and of the Council⁽²²⁾ (hereinafter referred to as the 'SEPA Regulation'), i.e. the consumer should have the right to instruct its account servicing payment service provider to establish specific positive or negative lists of TPPs⁽²³⁾.
- 2.9. In the context of direct debits, the proposed directive indicates that the payer should have an unconditional right to a refund, except where the payee has already fulfilled its contractual obligations and the services have already been received or the goods have been consumed by the payer⁽²⁴⁾. Instead of strengthening consumer protection, it appears likely that the proposed directive would no longer allow the unlimited refund rights under the current SEPA direct debit scheme. To comply with these provisions on the refund right, payment service providers would probably have to collect information about their customers' purchases. This is an issue which might raise concerns over privacy, as well as increasing the administrative burden on payment service providers. The ECB would instead suggest introducing, as a general rule, an unconditional refund right for a period of eight weeks for all consumer direct debits. For certain kinds of goods and services, debtors and creditors should be able to agree separately that no refund rights will apply. The Commission could establish an exhaustive list of such goods and services by delegated acts.
- 2.10. The financial compensation to be paid by the TPPs to the account servicing payment service provider in respect of unauthorised payment transactions pursuant to Articles 65 and 82 of the proposed directive does not correspond to compensation for non-execution, defective or late execution. The ECB would therefore suggest aligning these provisions with each other to ensure similar rules for compensation⁽²⁵⁾.
- 2.11. The existing PSD has contributed to a considerable extent to increasing the efficiency of retail payments by introducing the 'D+1' execution time for credit transfers⁽²⁶⁾. The ECB has observed that developments in business practices and technology allow for increasingly faster payment execution and welcomes that such services are already available in several Member States to the benefit of both consumers and enterprises. The ECB expects that the markets will continue to improve execution times across Europe and is pleased to support this process in its role as a catalyst.

⁽²¹⁾ See Article 58 of the proposed directive.

⁽²²⁾ See Recital 13, and Article 5(3)(d)(iii) of Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009 (OJ L 94, 30.3.2012, p. 22) (hereinafter the 'Single European Payments Area (SEPA) Regulation').

⁽²³⁾ See Articles 45 and 59 (new) of the proposed directive.

⁽²⁴⁾ See Recital 57 and Article 67(1) of the proposed directive.

⁽²⁵⁾ See Articles 65, 80 and 82 of the proposed directive.

⁽²⁶⁾ Article 69(1) of the existing PSD provides for credit transfers to be credited to the payment service provider's account of the payee by close of business on the day following receipt of the payment order at the latest.

- 2.12. The assessment of security arrangements and incident notifications⁽²⁷⁾ for payment service providers is a core competence of prudential supervisors and central banks. The development of supervisory requirements in these areas should thus remain under the control of these authorities. However, under the PSD, there is a need to share information with the competent authorities, the ECB, and, where relevant, with the European Network and Information Security Agency (ENISA) and competent authorities under the NIS directive in the area of operational risks, including security risks. The EBA should be responsible for coordinating such information-sharing between the competent authorities of Member States, whereby the ECB will notify the members of the ESCB as regards relevant issues for payment systems and payment instruments.
- 2.13. The EBA should also develop guidelines addressed to competent authorities on complaint procedures⁽²⁸⁾ that will assist in harmonising procedures.
- 2.14. Certain provisions⁽²⁹⁾ only concern Member States' discretion regarding national payments transactions. Such rules do not appear to be in line with the aim of establishing a single market for payment services and should preferably be taken out.
- 2.15. Finally, there are separate provisions on access and use of payment account information by TPPs and by third party payment instrument issuers, i.e. when a payment card is issued by a TPP⁽³⁰⁾. These services are not essentially different, so the ECB would suggest merging these provisions since the former regime on access and use of payment account information by the TPP could also apply *mutatis mutandis* to third party payment instrument issuers.

Where the ECB recommends that the proposed directive be amended, specific drafting proposals are set out in the Annex accompanied by explanatory text to this effect.

Done at Frankfurt am Main, 5 February 2014.

The President of the ECB

Mario DRAGHI

⁽²⁷⁾ See Articles 85 and 86 of the proposed directive.

⁽²⁸⁾ See Article 88(1) of the proposed directive.

⁽²⁹⁾ See Article 35(2) and 56(2) of the proposed directive.

⁽³⁰⁾ See Articles 58 and 59 respectively.

ANNEX

Drafting proposals

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
Amendment 1	
Recital 6	
<p>(6) In recent years, the security risks related electronic payments have increased, which is due to the greater technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and the emerging types of payment services. As safe and secure payment services constitute a vital condition for a well-functioning payment services market, users of payment services should be adequately protected against such risks. Payment services are essential for the maintenance of vital economic and societal activities and therefore payment services providers such as credit institutions have been qualified as market operators according to Article 3(8) of Directive [number of NIS Directive after adoption] of the European Parliament and of the Council ⁽²⁾.</p>	<p>(6) In recent years, the security risks related electronic payments have increased, which is due to the greater technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and the emerging types of payment services. As safe and secure payment services constitute a vital condition for a well-functioning payment services market, users of payment services should be adequately protected against such risks. Payment services are essential for the maintenance of vital economic and societal activities and therefore payment services providers such as credit institutions have been qualified as market operators according to Article 3(8) of Directive [number of NIS Directive after adoption] of the European Parliament and of the Council ⁽²⁾.</p>
<i>Explanation</i>	
<i>See Amendment 31.</i>	
Amendment 2	
Recital 7	
<p>(7) In addition to the general measures to be taken at Member States' level in Directive [pls insert number of NIS Directive after adoption], the security risks related to payment transactions should also be addressed at the level of the payment service providers. The security measures to be taken by the payment service providers need to be proportionate to the security risks concerned. A regular reporting mechanism should be established, so as to ensure payment services should provide the competent authorities on an annual basis with updated information on the assessment of their security risks and the (additional) measures that they have taken in response to these risks. Furthermore, in order to ensure that damages to other payment service providers and payment systems, such as a substantial disruption of a payment system and to users is kept to a minimum, it is essential that payment service providers have the obligation to report within undue delay major security incidents to the European Banking Authority.'</p>	<p>(7) In addition to the general measures to be taken at Member States' level in Directive [pls insert number of NIS Directive after adoption], The security risks related to payment transactions should also be addressed at the level of the payment service providers. The security measures to be taken by the payment service providers need to be proportionate to the security risks concerned. A regular reporting mechanism should be established, so as to ensure that payment services should provide the competent authorities on an annual basis with updated information on the assessment of their security risks and the (additional) measures that they have taken in response to these risks. Furthermore, in order to ensure that damages to other payment service providers and payment systems, such as a substantial disruption of a payment system and to users is kept to a minimum, it is essential that payment service providers have the obligation to report within without undue delay major operational and security incidents to the competent authority in the home Member State under this Directive, which shall assess the relevance of the incident for other authorities and, based on that assessment, shall share the relevant details of the incident notification with EBA and the ECB, which shall notify the competent authorities of other Member States and the ESCB.</p>

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
---------------------------------	---

Explanation

See Amendment 31.

Amendment 3

Recital 18

<p>(18) Since the adoption of Directive 2007/64/EC new types of payment services have emerged, especially in the area of internet payments. In particular, third party providers (hereinafter “TPPs”) have evolved, offering so-called payment initiation services to consumers and merchants, often without entering into the possession of the funds to be transferred. Those services facilitate the e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the consumer in order to initiate internet payments on the basis of credit transfers or direct debits. The TPPs offer a low-cost alternative to card payments for both merchants and consumers and provide consumers a possibility to shop online even if they do not possess credit cards. However, as TPPs are currently not subject to Directive 2007/64/EC, they are not necessarily supervised by a competent authority and do not follow the requirements of Directive 2007/64/EC. This raises a series of legal issues, such as consumer protection, security and liability as well as competition and data protection issues. The new rules should therefore respond to those issues.’</p>	<p>(18) Since the adoption of Directive 2007/64/EC new types of payment services have emerged, especially in the area of internet payments. In particular, third party providers (hereinafter “TPPs”) have evolved, offering so-called payment initiation services or account information services to consumers, and merchants and other payment service users, often without entering into the possession of the funds to be transferred. Payment initiation services facilitate the e-commerce payments by establishing a software bridge between the website of the merchant and the online banking platform of the consumer in order to initiate internet payments on the basis of credit transfers or direct debits. initiating, at the customers request, a payment order with respect to an account held at another payment service provider, for example via a connection to the customers online banking platform or by issuing a payment instrument. Account information services provide the payer with consolidated information on one or several accounts held by the payer with one or several other payment service providers. TPPs may also provide both payment initiation and account information services. The TPPs offer a low-cost alternative to card traditional payments for both merchants and consumers and provide consumers a possibility to shop online even if they do not possess credit cards. However, as TPPs are currently not subject to Directive 2007/64/EC, they are not necessarily supervised by a competent authority and do not follow the requirements of Directive 2007/64/EC. This raises a series of legal issues, such as consumer protection, security and liability as well as competition and data protection issues. The new rules should therefore respond to those issues.’</p>
---	---

Explanation

It is suggested to describe all types of TPPs under the same recital, therefore recitals 18 and 26 have been merged and reference is also made to TPPs issuing payment instruments, e.g. debit or credit cards. Following the inclusion of the latter, it is suggested to delete the example on the alternative to such cards. Moreover, the possibility is expressed that account information services could be provided at the same time as payment initiation services.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
---------------------------------	---

Amendment 4

Recital 26

<p>(26) With technological developments a range of complementary services have also emerged in recent years, such as account information and account aggregation services. These services should also be covered by this Directive in order to provide consumers with adequate protection and legal certainty about their status.'</p>	<p>(26) With technological developments a range of complementary services have also emerged in recent years, such as account information and account aggregation services. These services should also be covered by this Directive in order to provide consumers with adequate protection and legal certainty about their status.'</p>
--	---

Explanation

This recital has been merged with recital 18 (see Amendment 3).

Amendment 5

Recital 51

<p>(51) It is necessary to set up the criteria under which TPPs are allowed to access and use the information on the availability of funds on the payment service user account held with another payment service provider. In particular, necessary data protection and security requirements set or referred to in this Directive or included in the EBA guidelines should be fulfilled by both the TPP and the payment service provider servicing the account of the payment service user. The payers should give an explicit consent to the TPP to access their payment account and be properly informed about the extent of this access. To allow the development of other payment services providers which cannot receive deposits, it is necessary that credit institutions provide them with the information on the availability of funds if the payer has given consent for this information to be communicated to the payment service provider issuer of the payment instrument.'</p>	<p>(51) It is necessary to set up the criteria under which TPPs are allowed to access and use the information on the availability of funds on the payment service user account held with another payment service provider. In particular, necessary data protection and security requirements set or referred to in this Directive or included in the EBA guidelines should be fulfilled by both the TPP and the payment service provider servicing the account of the payment service user. The payers payment service users should give an explicit consent to the TPP to access their payment account and be properly informed about the extent of this access. To allow the development of other new payment service providers which cannot receive deposits do not hold funds of the payer, it is necessary that credit institutions account-holding payment service providers provide them the TPP with the information on the availability of funds if the payer payment service user has given consent for this information to be communicated to the TPP issuer of the payment instrument.'</p>
--	---

Explanation

Editorial clarification on parties concerned.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
Amendment 6	
Recital 52	
<p>(52) Rights and obligations of the payment service users and payment service providers should be appropriately adjusted to take account of the TPP involvement in the transaction whenever the payment initiation service is used. Specifically, a balanced liability repartition between the payment service provider servicing the account and the TPP involved in the transaction should compel them to take responsibility for the respective parts of the transaction that are under their control and clearly point to the responsible party in case of incidents. In case of fraud or dispute, the TPP should be under a specific obligation to provide the payer and the account servicing payment service provider with the reference of the transactions and the information of the authorisation relating to the transaction concerned.'</p>	<p>(52) Rights and obligations of the payment service users and payment service providers should be appropriately adjusted to take account of the TPP involvement in the transaction whenever the payment initiation service is used. Specifically, a balanced liability repartition between the payment service provider servicing the account and the TPP involved in the transaction should compel them to take responsibility for the respective parts of the transaction that are under their control and clearly point to the responsible party in case of incidents. In case of fraud or dispute, the TPP should be under a specific obligation to provide the payer payment service users and the account servicing payment service provider with the reference of the transactions and the information of the authorisation relating to the transaction concerned proof that the payment service users have been authenticated.'</p>

Explanation

See Amendment 19 and 24.

Amendment 7	
Recital 57	
<p>(57) This Directive should lay down rules for a refund to protect the consumer when the executed payment transaction exceeds the amount which could reasonably have been expected. In order to prevent a financial disadvantage for the payer, it needs to be ensured that the credit value date of any refund is no later than the date when the respective amount has been debited. In the case of direct debits payment service providers should be able to provide even more favourable terms to their customers, who should have an unconditional right to a refund of any disputed payment transactions. However, this unconditional refund right which ensures the highest level of consumer protection is not justified in cases where the merchant has already fulfilled the contract and the corresponding good or service has already been consumed. In cases where the user makes a claim for the refund of a payment transaction refund rights should affect neither the liability of the payer vis-à-vis the payee from the underlying relationship, e.g. for goods or services ordered, consumed or legitimately charged, nor the users rights with regard to revocation of a payment order.'</p>	<p>(57) This Directive should lay down rules for a refund to protect the consumer when the executed payment transaction exceeds the amount which could reasonably have been expected. In order to prevent a financial disadvantage for the payer, it needs to be ensured that the credit value date of any refund is no later than the date when the respective amount has been debited. In the case of direct debits payment service providers should be able to provide even more favourable terms to their customers, who should have an unconditional right to a refund of any disputed payment transactions. However, this unconditional refund right which ensures the highest level of consumer protection is not justified in cases where the merchant has already fulfilled the contract and the corresponding good or service has already been consumed for certain kinds of goods or services an unconditional refund right might not be appropriate. The possibility of introducing a no-refund direct debit may therefore be considered, but only for goods or services set out by the Commission on a list and only with the payer's explicit consent. In cases where the user makes a claim for the refund of a payment transaction refund rights should affect neither the liability of the payer vis-à-vis the payee from the underlying relationship, e.g. for goods or services ordered, consumed or legitimately charged, nor the users rights with regard to revocation of a payment order.'</p>

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
<i>Explanation</i>	
<p><i>Making refund rights dependent on the underlying purchase raises privacy concerns, as well as concerns relating to efficiency and costs. The adoption of this proposal would probably mean that the unlimited refund rights under the current SEPA direct debit scheme would no longer be permitted, bringing less favourable conditions to consumers. The ECB suggests introducing, as a general rule, an unconditional refund right for a period of eight weeks for all consumer direct debits. For listed goods or services meant for immediate consumption, debtors and creditors could separately and explicitly agree that no refund rights should apply. The Commission could establish such a list by means of a delegated act.</i></p>	
Amendment 8	
Recital 80	
<p>'(80) In order to ensure consistent application of this Directive, the Commission should be able to rely on the expertise and support of EBA, which should have the task to elaborate guidelines and prepare regulatory technical standards on security aspects regarding payment services, and on the cooperation between Member States in the context of the provision of services and establishment of authorised payment institutions in other Member States. The Commission should be empowered to adopt those regulatory technical standards. These specific tasks are fully in line with the role and responsibilities of EBA defined in Regulation (EU) No 1093/2010, under which the EBA has been set up.'</p>	<p>'(80) In order to ensure consistent application of this Directive, the Commission should be able to rely on the expertise and support of EBA, which should, in close cooperation with the ECB, have the task to elaborate guidelines and prepare regulatory technical standards on security aspects regarding payment services, and on the cooperation between Member States in the context of the provision of services and establishment of authorised payment institutions in other Member States. The Commission should be empowered to adopt those regulatory technical standards. These specific tasks are fully in line with the role and responsibilities of EBA defined in Regulation (EU) No 1093/2010, under which the EBA has been set up.'</p>
<i>Explanation</i>	
<p><i>Security aspects with respect to payment services also fall under the competence of central banks. The ECB has established, on a voluntary basis, a close cooperation with supervisors of payment service providers in the SecuRe Pay Forum. This successful cooperation should be formalised. The current proposal does not include any regulatory technical standards; therefore the reference has been deleted.</i></p>	
Amendment 9	
Article 2	
<p>1. This Directive shall apply to payment services provided within the Union, where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located therein. Article 78 and Title III shall also apply to payment transactions where only one of the payment service providers is located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.</p> <p>2. Title III shall apply to payment services in any currency. Title IV shall apply to payment services made in euro or the currency of a Member State outside the euro area.'</p>	<p>1. This Directive shall apply to payment services provided within the Union, where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located therein. Article 78 and Title III and Title IV, except for Articles 72 and 74(1), shall also apply to payment transactions where only one of the payment service providers is located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.</p> <p>2. Titles III and IV shall apply to payment services in any currency. Title IV shall apply to payment services made in euro or the currency of a Member State outside the euro area.'</p>

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
<i>Explanation</i>	
<i>In order to ensure comprehensive protection to users of payment services, the provisions on transparency and credit value date, as well as the provisions on rights and obligations relating to the provision and use of payment services should apply to transactions where only one of the payment service providers is located within the Union, in respect to those parts of the transaction that are carried out in the Union.</i>	
Amendment 10	
Article 4(32)	
<p>'32. "payment initiation service" means a payment service enabling access to a payment account provided by a third party payment service provider, where the payer can be actively involved in the payment initiation or the third party payment service provider's software, or where payment instruments can be used by the payer or the payee to transmit the payer's credentials to the account servicing payment service provider;'</p>	<p>'32. "payment initiation service" means a payment service enabling access to initiate a payment account order provided by a third party payment service provider, at the request of the payer, with respect to an account held at another where the payer can be actively involved in the payment initiation or the third party payment service provider's software, or where payment instruments can be used by the payer or the payee to transmit the payer's credentials to the account servicing payment service provider;'</p>
<i>Explanation</i>	
<i>The definition needs to remain as simple and flexible as possible so that future solutions are also covered. The definition should be free of requirements or references to specific technologies.</i>	
Amendment 11	
Article 4(33)	
<p>'33. "account information service" means a payment service where consolidated and user-friendly information is provided to a payment service user on one or several payment accounts held by the payment service user with one or several account servicing payment service providers;'</p>	<p>'33. "account information service" means a payment service provided by a third party payment service provider where consolidated and user friendly information is provided to a payment service user on one or several payment accounts held by the payment service user with one or several account servicing payment service providers to provide consolidated information on one or several payment accounts held by the payment service user with one or several other payment service providers;'</p>
<i>Explanation</i>	
<i>The definition needs to remain as simple and flexible as possible so that future solutions are also covered. The definition should be free of requirements or references to specific technologies.</i>	
Amendment 12	
Article 4(39)-(43) (new)	
<p>No text</p>	<p>'39. "acquiring of payment transactions" means a payment service provided by a payment service provider contracting with a payee to accept and process the payee's payment transactions initiated by a payer's payment instrument, which result in a transfer of funds to the payee; the service could include providing authentication, authorisation, and other services related to the management of financial flows to the payee regardless of whether the payment service provider holds the funds on behalf of the payee;</p>

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
	<p>40. “issuing of payment instruments” means a payment service where a payment service provider directly or indirectly provides the payer with a payment instrument to initiate, process and settle the payer’s payment transactions;</p> <p>41. “credit transfer” means a national or cross-border payment service for crediting a payee’s payment account with a payment transaction or a series of payment transactions from a payer’s payment account by the PSP which holds the payer’s payment account, based on an instruction given by the payer;</p> <p>42. “cross-border payment” means an electronically processed payment transaction initiated by a payer or through a payee where the payer’s payment service provider and the payee’s payment service provider are located in different Member States;</p> <p>43. “national payment” means an electronically processed payment transaction initiated by a payer, or by or through a payee, where the payer’s payment service provider and the payee’s payment service provider are located in the same Member State.’</p>

Explanation

The definitions of ‘issuing of payment instruments’ and ‘acquiring payment transactions’ should be added in order to ensure that all providers involved in payment services come under the proposed directive as provided for in Annex I. These definitions should be aligned with the proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions (COM (2013) 550/3); 2013/0265.

The definition of ‘credit transfer’ should be included since this is one of the core payment instruments of the abovementioned proposed regulation. The inserted definition is aligned with the SEPA Regulation. Including definitions for ‘cross-border payment’ and ‘national payment’ should increase clarity.

Amendment 13

Article 9(1) introductory paragraph

<p>‘1. The Member States or competent authorities shall require a payment institution which provides any payment services and, insofar as it at the same time is engaged in other business activities referred to in Article 17(1)(c) to safeguard all funds which have been received from the payment service users or through another payment service provider for the execution of payment transactions, in either of the following ways:’</p>	<p>‘1. The Member States or competent authorities shall require a payment institution which provides any payment services and, insofar as it at the same time is engaged in other business activities referred to in Article 17(1)(c) to safeguard all funds which have been received from the payment service users or through another payment service provider for the execution of payment transactions, in either of the following ways:’</p>
---	--

Explanation

In line with the aim to harmonise safeguarding requirements, the alternative text is suggested in order to ensure that payment service user’s funds for all payment institutions are appropriately protected, regardless of whether they are engaged in other business activities.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
Amendment 14	
Article 12(1)	
<p>‘1. The competent authorities may withdraw an authorisation issued to a payment institution only where the institution falls within the following cases:</p> <p>[...]</p> <p>(c) no longer fulfils the conditions for granting the authorisation or fails to inform the competent authority on major developments in this respect;’</p>	<p>‘1. The competent authorities may withdraw an authorisation issued to a payment institution only where the institution falls within the following cases:</p> <p>[...]</p> <p>(c) no longer fulfils the conditions for granting the authorisation or fails to inform the competent authority on major developments in this respect or to provide accurate statistical reporting;’</p>

Explanation

Providing accurate statistical information is essential for monitoring risk related to payment institutions.

Amendment 15	
Article 25(2)	
<p>‘2. Member States shall, in addition, allow the exchange of information between their competent authorities and the following:</p> <p>(a) the competent authorities of other Member States responsible for the authorisation and supervision of payment institutions;</p> <p>(b) the European Central Bank and the national central banks of Member States, in their capacity as monetary and oversight authorities, and, where appropriate, other public authorities responsible for overseeing payment and settlement systems;</p> <p>(c) other relevant authorities designated under this Directive, Directive 2005/60/EC and other Union legislation applicable to payment service providers, such as legislation applicable to money laundering and terrorist financing;</p> <p>(d) EBA, in its capacity of contributing to the consistent and coherent functioning of supervising mechanisms as referred to in Article 1(5)(a) of Regulation (EU) 1093/2010.’</p>	<p>‘2. Member States shall, in addition, allow the exchange of information between their competent authorities and the following:</p> <p>(a) the competent authorities of other Member States responsible for the authorisation and supervision of payment institutions;</p> <p>(b) the European Central Bank and the national central banks of Member States, in their capacity as monetary and oversight authorities, and, where appropriate, other public authorities responsible for overseeing payment and settlement systems;</p> <p>(c) other relevant authorities designated under this Directive, Directive 2005/60/EC and other Union legislation applicable to payment service providers, such as legislation applicable to money laundering and terrorist financing;</p> <p>(d) EBA, in its capacity of contributing to the consistent and coherent functioning of supervising mechanisms as referred to in Article 1(5)(a) of Regulation (EU) 1093/2010, and where appropriate;</p> <p>(e) Europol, in its capacity as the Union’s law enforcement agency responsible for assisting and coordinating a common approach among competent police authorities of the Member States in combatting organised and other serious crime and terrorism including euro counterfeiting, forgery of money and other means of payment.’</p>

Explanation

Europol should be added as an additional authority with which the competent authorities should be able to share information, in view of its competence and expertise in investigating and coordinating, at Union level, the fight against, inter alia, euro counterfeiting, forgery and other serious financial crime involving means of payment. See Annex to Council Decision 2009/371/JHA ⁽³⁾.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
Amendment 16	
Article 27(5)(a) (new)	
No text	'5. (a) Natural or legal persons pursuing business activities referred to in point 7 of Annex I should not be subject to any waiver.'
<i>Explanation</i>	
<i>Since account servicing payment service providers have to provide access to TPPs, allowing the latter to obtain a waiver from the supervisory requirements could bring unanticipated risks. Additionally, the services that TPPs offer are usually provided over the internet and therefore not limited to one single Member State. Therefore, TPPs should not be able to obtain a waiver.</i>	
Amendment 17	
Article 35(2)	
'2. For national payment transactions, Member States or their competent authorities may reduce or double the amounts referred to in paragraph 1. For prepaid payment instruments, Member States may increase those amounts up to EUR 500.'	'2. For national payment transactions, Member States or their competent authorities may reduce or double the amounts referred to in paragraph 1. For prepaid payment instruments, Member States may increase those amounts up to EUR 500.'
<i>Explanation</i>	
<i>For national payment transactions, i.e. those that are not cross-border, it does not appear necessary to allow Member States or their competent authorities to significantly adjust the maximum payment amounts in Article 35(1) due to the derogation for low value payment instruments. Additionally, allowing this adjustment would result in very divergent national regimes on derogation, which conflicts with the objective of an integrated and harmonised European retail payments market.</i>	
Amendment 18	
Article 39	
'(d) where applicable, the amount of any charges for the payment transaction and, where applicable, a breakdown thereof.'	'(d) where applicable, the amount of any charges for the payment transaction payable to the third party payment service provider for the transaction , and, where applicable, a breakdown of the amounts of such charges.
<i>Explanation</i>	
<i>This addition provides clarification that with regard to charges, third party payment services providers will only be able to detail their own charges; not charges levied by the account servicing payment services provider.</i>	
Amendment 19	
Article 40	
'Where a payment order is initiated by the third party payment service provider's own system, it shall in case of fraud or dispute make available to the payer and the account servicing payment service provider the reference of the transactions and the authorisation information.'	'Where a payment order is initiated by the third party payment service provider's own system, it shall in case of fraud or dispute make available to the payer and the account servicing payment service provider the reference of the transactions and the authorisation information proof that the user has been authenticated in accordance with Article 58(2).'

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
---------------------------------	---

Explanation

Since personalised security features should no longer be shared, the TPP in the event of a dispute or fraud needs to prove that (a) the PSP confirmed to the TPP that the transaction has been authorised or (b) that the customer was undisputedly authenticated based on the personalised security features issued by the TPP.

Amendment 20

Article 41

'Immediately after receipt of the payment order, the payer's payment service provider shall provide or make available to the payer, in the same way as provided for in Article 37(1), the following data: [...].'

'Immediately after receipt of the payment order, the **account servicing payer's** payment service provider shall provide or make available to the payer, in the same way as provided for in Article 37(1), the following data: [...].'

Explanation

This change provides clarification that this article refers only to account servicing payment service providers, since the TPPs' obligations are already outlined in Article 39. This applies to situations where TPPs are involved as well as for traditional payment services.

Amendment 21

Article 45(5)(g) (new)

No text

'(g) **information from the payment service provider on the payment service user's right to block any payment initiation service from the payment service user's account, or establish positive or negative lists of TPPs.**'

Explanation

Payment service users will only be able to exercise their rights under proposed Article 59 (new) to block payment initiation services or to establish positive or negative lists for specific TPPs if they are informed accordingly.

Amendment 22

Article 54(1)

'1. Where the payment service user is not a consumer, the payment service user and the payment service provider may agree that Article 55(1), Article 57(3), and Articles 64, 66, 67, 68, 71 and 80 shall not apply in whole or in part. The payment service user and the payment service provider may also agree on a time period different from that laid down in Article 63.'

'1. Where the payment service user is not a consumer, the payment service user and the payment service provider may agree that Article 55(1), Article 57(3), and Articles **59** (new), 64, 66, 67, 68, 71 and 80 shall not apply in whole or in part. The payment service user and the payment service provider may also agree on a time period different from that laid down in Article 63.'

Explanation

See explanation to Amendment 26.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
Amendment 23	
Article 56(2)	
<p>'2. For national payment transactions, Member States or their competent authorities may reduce or double the amounts referred to in paragraph 1. They may increase them for prepaid payment instruments up to EUR 500.'</p>	<p>'2. For national payment transactions, Member States or their competent authorities may reduce or double the amounts referred to in paragraph 1. They may increase them for prepaid payment instruments up to EUR 500.'</p>

Explanation

For national payment transactions, i.e. those that are not cross-border, it does not appear necessary to allow Member States or their competent authorities to significantly adjust the maximum payment amounts in Article 56(1) due to the derogation for low value payment instruments. Additionally, allowing this adjustment would result in very divergent national regimes on derogation, which conflicts with the objective of an integrated and harmonised European retail payments market.

Amendment 24	
Article 58	
<p>'1. Member States shall ensure that a payer has the right to make use of a third party payment service provider to obtain payment services enabling access to payment accounts as referred to in point (7) of Annex I.</p> <p>2. Where a third party payment service provider has been authorised by the payer to provide payment services under paragraph 1, he shall have the following obligations:</p> <p>(a) to ensure that the personalised security features of the payment service user are not accessible to other parties;</p> <p>(b) to authenticate itself in an unequivocal manner towards the account servicing payment service provider(s) of the account owner.</p>	<p>'1. Member States shall ensure that a payment service user has the right to make use of a third party payment service provider to obtain payment services enabling based on access to payment accounts as referred to in point (7) of Annex I.</p> <p>2. Where a third party payment service provider has been authorised by the payment service user to provide payment services under paragraph 1, it shall have the following obligations:</p> <p>(a) to ensure that the personalised security features of the payment service user are not accessible to other parties strong customer authentication for the initiation of payments or access to account information by:</p> <p style="padding-left: 40px;">i. redirecting the payment service user in a secure manner to its account servicing payment service provider for such authentication; or</p> <p style="padding-left: 40px;">ii. issuing its own personalised security features for such authentication.</p> <p>The third party payment service provider shall not be allowed to obtain the payment service user's personalised security features issued by the account servicing payment service provider.</p> <p>(b) to authenticate itself in an unequivocal manner towards the account servicing payment service provider(s) of the account owner payment service user.</p>

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
<p>(c) not to store sensitive payment data or personalised security credentials of the payment service user.</p> <p>3. Where, for a payment initiation service, the account servicing payment service provider has received the payer's payment order through the services of a third party payment service provider, it shall immediately notify the latter of the receipt of the payment order and provide information on the availability of sufficient funds for the specified payment transaction.</p> <p>4. Account servicing payment service providers shall treat payment orders transmitted through the services of a third party payment service provider without any discrimination for other than objective reasons in terms of timing and priority vis-à-vis payment orders transmitted directly by the payer himself.</p>	<p>(c) not to store sensitive payment data or personalised security credentials of the payment service user obtained when accessing the payment service users payment account, apart from information for identifying a payment initiated by the third party payment service provider such as the reference number, payer's and payee's IBAN, the transaction amount, other reference information and the settlement system information, and not use any data for other purposes than explicitly requested by the payment service user.</p> <p>3. Member States shall ensure that account servicing payment service providers provide facilities to receive payment orders from third party payment service providers and to accept a redirection as stated under paragraph (2) of this article</p> <p>4.3. Where, for a payment initiation service, the payment order is transmitted through the services of a third party payment service provider, the account servicing payment service provider has received the payer's payment order through the services of a third party payment service provider, it shall immediately notify the latterformer of the receipt delivery of the payment order and provide information on the availability of sufficient funds for the specified payment transaction.</p> <p>5.4. Account servicing payment service providers shall treat payment orders transmitted through the services of a third party payment service provider without any discrimination for other than objective reasons in terms of timing and priority vis-à-vis payment orders transmitted directly by the payer himself.</p> <p>6. Member States shall ensure that account servicing payment service providers shall offer, when available, a secure standardised interface for third party payment service based on access to payment accounts. The European standard should be based on a guideline defined by EBA within [...] of entry into force of this directive, in close cooperation with the ECB, and include, at a minimum, technical and functional specifications for transmitting a payment order between the account servicing payment service provider and the third party payment service provider under 2(a)(i), and for the unequivocal authentication of the third party payment service provider as stated under 2(b).</p>

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
---------------------------------	---

Explanation

It is a core principle of IT security that credentials used to authenticate the payment service user are not shared with any third party. Therefore TPPs should ensure strong customer authentication by either: (a) redirecting the payment service user in a secure manner to its account servicing payment service provider; or b) issuing its own personalised security features. Both options should form part of the standardised European technical interface for payment account access.

This secure standardised interface for third party service providers for access to payment account information should be based on an open European standard and allow, upon the transposition of the proposal, any TPP to access payment accounts at any PSP throughout the Union. This interface should be defined shortly after the proposed directive is adopted, by EBA in close cooperation with the ECB and include, at a minimum, technical and functional specifications as well as related procedures.

Furthermore, third party service providers should: (a) protect the personalised security features of the payment service user, (b) authenticate themselves in an unequivocal manner as regards the payment service user's account servicing payment service provider(s); (c) refrain from storing data obtained when accessing the payment service user's payment account, apart from information for identifying a payment initiated by TPPs, such as the reference number, payer's and payee's IBAN, the transaction amount; and (d) refrain from using any data for purposes other than explicitly requested by the payer.

Amendment 25

Article 59

<i>'Article 59</i>	<i>'Article 59</i>
<p style="text-align: center;">Access to and use of payment account information by third party payment instrument issuers</p> <ol style="list-style-type: none"> 1. Member States shall ensure that a payer has the right to make use of a third party payment instrument issuer to obtain payment card services. 2. If the payer has given consent to a third party payment instrument issuer which has provided the payer with a payment instrument to obtain information on the availability of sufficient funds for a specified payment transaction on a specified payment account held by the payer, the account servicing payment service provider of the specified payment account shall provide such information to the third party payment instrument issuer immediately upon receipt of the payer's payment order. 3. Account servicing payment service providers shall treat payment orders transmitted through the services of a third party payment instrument issuer without any discrimination for other than objective reasons in terms of timing and priority in respect of payment orders transmitted directly by the payer personally.' 	<p style="text-align: center;">Access to and use of payment account information by third party payment instrument issuers</p> <ol style="list-style-type: none"> 1. Member States shall ensure that a payer has the right to make use of a third party payment instrument issuer to obtain payment card services. 2. If the payer has given consent to a third party payment instrument issuer which has provided the payer with a payment instrument to obtain information on the availability of sufficient funds for a specified payment transaction on a specified payment account held by the payer, the account servicing payment service provider of the specified payment account shall provide such information to the third party payment instrument issuer immediately upon receipt of the payer's payment order. 3. Account servicing payment service providers shall treat payment orders transmitted through the services of a third party payment instrument issuer without any discrimination for other than objective reasons in terms of timing and priority in respect of payment orders transmitted directly by the payer personally.'

Explanation

The provisions of this article on the access to and use of payment account information by third party PSPs issuing payment instruments, e.g. payment cards are in substance identical to those of Article 58 governing the access to and use of payment account information by third party PSPs. Accordingly Article 59 could be deleted without any risk to legal certainty for PSPs and for payers making use of their services.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
---------------------------------	---

Amendment 26

Article 59 (new)

No text	<p>'Article 59. The payer must have the right to: (i) instruct its account servicing payment service provider to block any payment initiation services from the payer's payment account; (ii) to block any payment initiation services initiated by one or more specified third party payment service providers; or (iii) to only authorise payment initiation services initiated by one or more specified third party payment service providers.'</p>
---------	---

Explanation

In line with the provisions on consumer protection and the safeguards for payment service users contained in Recital 13 and Article 5(3)(d)(iii) of the SEPA Regulation, and to ensure legal consistency, a new article guaranteeing payment service users the right to instruct their PSPs to establish specific positive or negative lists of TPPs should be added. This provision should not, however, apply to payment users other than consumers (see Amendment 22). Since the instructions must come from the payer, this should not cover a generalised default blocking or inclusion of a generalised blocking of TPPs in the terms and conditions or contracts of a PSP.

Amendment 27

Article 65(2)

<p>'2. Where a third party payment service provider is involved, the account servicing payment service provider shall refund the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. Financial compensation to the account servicing payment service provider by the third party payment service provider may be applicable.'</p>	<p>'2. Where a third party payment service provider is involved, the account servicing payment service provider shall refund the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. Financial compensation to the account servicing payment service provider by the third party payment service provider may be applicable shall be provided in accordance with Article 82.'</p>
--	--

Explanation

From a customer protection perspective, it is natural that payer would turn to the account servicing payment service provider for a refund, since their relationship with the TPP may only take place on a one-off basis, e.g. for payment initiation. The account servicing payment service provider could then claim compensation from the TPP, unless the TPP can prove that it was not responsible for the error. Compensation for the TPP should follow the same rules as for the non-execution, defective or late execution of a payment transaction pursuant to Article 80 as well as a right of recourse pursuant to Article 82. Such compensation may, for example, be available where the TPP has issued its own security features, e.g. for a payment card.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
---------------------------------	---

Amendment 28

Article 66(1)

<p>‘1. By way of derogation from Article 65 the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.</p> <p>The payer shall bear all the losses relating to any unauthorised payment transactions if incurred by acting fraudulently or by failing to fulfil one or more of the obligations set out in Article 61 with intent or gross negligence. In such cases, the maximum amount referred to in paragraph 1 of this Article shall not apply. For payments via a distance communication where the payment service provider does not require strong customer authentication, the payer shall only bear any financial consequences where having acted fraudulently. Should the payee or the payment service provider of the payee fail to accept strong customer authentication, they shall refund the financial damage caused to the payer’s payment service provider.’</p>	<p>‘1. By way of derogation from Article 65 the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.</p> <p>The payer shall bear all the losses relating to any unauthorised payment transactions if incurred by acting fraudulently or by failing to fulfil one or more of the obligations set out in Article 61 with intent or gross negligence. In such cases, the maximum amount referred to in paragraph 1 of this Article shall not apply. For payments via a distance communication where the payment service provider does not require strong customer authentication, the payer shall only bear any financial consequences where having acted fraudulently. Should the payee or the payment service provider of the payee fail to accept strong customer authentication, they shall refund the financial damage caused to the payer’s payment service provider.’Where the payment service provider does not require strong customer authentication, the payer shall only bear any financial consequences where having acted fraudulently. Should the payee or the payment service provider of the payee fail to accept strong customer authentication, they shall refund the financial damage caused to the payer’s payment service provider.’</p>
--	--

Explanation

Consumers should be ensured similar protection irrespective of the payment initiation channel.

Amendment 29

Article 67(1)

<p>‘1. Member States shall ensure that a payer is entitled to a refund from the payment service provider of an authorised payment transaction initiated by or through a payee which has already been executed, if the following conditions are met:</p> <p>[...]For direct debits the payer has an unconditional right for refund within the time limits set in Article 68, except where the payee has already fulfilled the contractual obligations and the services have already been received or the goods have already been consumed by the payer. At the payment service provider’s request, the payee shall bear the burden to prove that the conditions referred to in the third subparagraph.’</p>	<p>‘1. Member States shall ensure that a payer is entitled to a refund from the payment service provider of an authorised payment transaction initiated by or through a payee which has already been executed, if the following conditions are met:</p> <p>[...]For direct debits the payer has an unconditional right for refund within the time limits set in Article 68; except where the payee has already fulfilled the contractual obligations and the services have already been received or the goods have already been consumed by the payer. The Commission may, however, by delegated acts establish an exhaustive list of goods and services that may be provided subject to a no-refund direct debit. The payer and payee shall be required to agree separately on a no-refund direct debit in respect of any such listed goods and services and to clearly mention the absence of the unconditional refund right in the mandate. At the payment service provider’s request, the payee shall bear the burden to prove that the conditions referred to in the third subparagraph are fulfilled.’</p>
--	--

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
<i>Explanation</i>	
<p>Making refund rights dependent on the underlying purchase raises privacy concerns, as well as concerns relating to efficiency and costs. The adoption of this proposal would probably mean that the unlimited refund rights under the current SEPA direct debit scheme would no longer be permitted, bringing less favourable conditions to consumers. The ECB suggests introducing, as a general rule, an unconditional refund right for a period of eight weeks for all consumer direct debits. For listed goods or services meant for immediate consumption, debtors and creditors could separately and explicitly agree that no refund rights should apply. The Commission could establish such a list by means of a delegated act.</p>	

Amendment 30

Article 82(1)

<p>'1. Where the liability of a payment service provider under Article 80 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid under Article 80. This shall include compensation where any of the payment service providers fail to use strong customer authentication.'</p>	<p>'1. Where the liability of a payment service provider under Article 65 and Article 80 is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid under Article 65 and Article 80. This shall include compensation where any of the payment service providers fail to use strong customer authentication.'</p>
---	---

Explanation

Unauthorised payment transactions should also be covered under the right of recourse. In order to provide more clarity, it would be desirable to define the term 'intermediary' in the proposed directive.

Amendment 31

Article 85

'Article 85 Security requirements and incident notification	'Article 85 Security requirements and incident notification
<p>1. Payment service providers are subject to Directive [NIS Directive] and notably to the risk management and incident reporting requirements in Articles 14 and 15 therein.</p> <p>2. The authority designated under Article 6(1) of Directive [NIS Directive] shall without undue delay inform the competent authority in the home Member State and EBA of the notifications of NIS incidents received from payment services providers.</p>	<p>1. Payment service providers are subject to Directive [NIS Directive] and notably to the risk management and incident reporting requirements in Articles 14 and 15 therein. Payment service providers shall establish a framework with appropriate mitigation measures and control mechanisms to manage the operational risks, including security risks, related to the payment services they provide. As part of this framework payment service providers shall define and maintain effective incident management procedures, including the classification of major incidents.</p> <p>2. The authority designated under Article 6(1) of Directive [NIS Directive] shall without undue delay inform the competent authority in the home Member State and EBA of the notifications of NIS incidents received from payment services providers. In the case of a major operational incident, including security incidents, payment service providers shall, without undue delay, notify the competent authority in the home Member State under this Directive about the incident.</p>

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
<p>3. Upon receipt of the notification, and where relevant, EBA shall notify the competent authorities in the other Member States.</p> <p>4. In addition to the provisions of Article 14(4) of Directive [NIS Directive], where the security incident has the potential of impacting the financial interests of the payment service users of the payment service provider, it shall without undue delay notify its payment service users of the incident and inform them of possible mitigation measures that they can take on their side to mitigate the adverse effects of the incident.'</p>	<p>3. Upon receipt of the notification, and where relevant, EBA shall notify the competent authorities in the other home Member States under this Directive shall assess the relevance of the incident for other authorities, and based on that assessment shall share the relevant details of the incident notification with EBA and the European Central Bank.</p> <p>4. Upon receipt of the notification, and where relevant, EBA shall notify the competent authorities of other Member States under this Directive. The ECB shall notify the ESCB on relevant issues for payment systems and payment instruments.</p> <p>5.4. In addition to the provisions of Article 14(4) of Directive [NIS Directive], wWhere the security incident has the potential of impacting the financial interests of the payment service users of the payment service provider, it shall without undue delay notify its payment service users of the incident and inform them of the possible mitigation measures that they can take on their side to mitigate the adverse effects of the incident.</p> <p>6. By the [insert date] EBA shall in close cooperation with the ECB issue guidelines in accordance with the procedure laid down in Article [insert number] of Directive [insert number of Directive] for payment service providers on the classification of major incidents referred to in paragraph 1, on the content, the format and the procedures of incident notifications referred to in paragraph 2, and for the competent authorities under this Directive with regard to the criteria on how to assess which incident notifications are of relevance for other authorities, and which details of the incident reports shall be shared with the other authorities.</p> <p>7. EBA shall in close cooperation with the ECB review the guidelines referred to in paragraph 6 on a regular basis, but at least every two years.</p> <p>8. While issuing and reviewing the guidelines referred to in paragraph 6 EBA may consider the Commission's implementing act in accordance with Article 14(7) of Directive [NIS Directive] and standards and/or specifications developed and published by European Union Agency for Network and Information Security for sectors pursuing activities other than payment service provision.'</p>

Text proposed by the Commission

Amendments proposed by the ECB⁽¹⁾

Explanation

Supervisors and the ESCB are the competent authorities to issue guidelines on incident management and incident notifications for payment service providers as well as to issue guidelines on sharing incident notifications between the relevant authorities. Placing payment service providers under the NIS Directive could interfere with the tasks of supervisory authorities and central banks, and should therefore be avoided. However, guidelines developed by ENISA for other sectors and the requirements to be laid down in the Commission's implementing act in accordance with Article 14(7) of the proposed NIS Directive could be considered in order to ensure a reasonable level of consistency between sector-specific pieces of legislation. The mandate for issuing the guidelines on the classification of incidents and incident reporting is closely related to the requirements laid down in this Article. Therefore it is suggested that the mandate forms part of this Article rather than Article 86.

Amendment 32

Article 86

**'Article 86
Implementation and reporting**

1. Member States shall ensure that payment service providers provide to the authority designated under Article 6(1) of Directive [NIS Directive] on a yearly basis updated information of the assessment of the operational and security risks associated with the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to these risks. The authority designated under Article 6(1) of Directive [NIS Directive] shall without undue delay transmit a copy of this information to the competent authority in the home Member State.
2. Without prejudice to Articles 14 and 15 of Directive [NIS Directive], EBA shall, in close cooperation with the ECB, develop guidelines with regard to the establishment, implementation and monitoring of the security measures, including certification processes when relevant. It shall, *inter alia*, take into account the standards and/or specifications published by the Commission under Article 16(2) of Directive [NIS Directive].
3. EBA shall, in close cooperation with the ECB, review the guidelines on a regular basis, but at least every two years.

**'Article 86
Implementation and reporting**

1. Member States shall ensure that payment service providers provide to the **competent authority under this Directive** ~~designated under Article 6(1) of Directive [NIS Directive]~~ on a yearly basis updated information of the assessment of the operational and security risks associated with the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to these risks. ~~The authority designated under Article 6(1) of Directive [NIS Directive] shall without undue delay transmit a copy of this information to the competent authority in the home Member State.~~
2. ~~Without prejudice to Articles 14 and 15 of Directive [NIS Directive],~~ EBA shall, in close cooperation with the ECB, develop guidelines **for payment service providers** with regard to the establishment, implementation and monitoring of the security measures, including certification processes when relevant. It shall, *inter alia*, take into account the standards and/or specifications published by the Commission under Article 16(2) of Directive [NIS Directive].
3. EBA shall, in close cooperation with the ECB, review the guidelines on a regular basis, but at least every two years.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
<p>4. Without prejudice to Articles 14 and 15 of Directive [NIS Directive], EBA shall issue guidelines to facilitate payment service providers in qualifying major incidents and the circumstances under which a payment institution is required to notify a security incident. Those guidelines shall be issued by (insert date - two years of the date of entry into force of this Directive).'</p>	<p>4. EBA shall coordinate the sharing of information in the area of operational and security risks associated with payment services with the competent authorities under this Directive, the ECB, the competent authorities under the NIS Directive, and where relevant, with ENISA.</p> <p>Without prejudice to Articles 14 and 15 of Directive [NIS Directive], EBA shall issue guidelines to facilitate payment service providers in qualifying major incidents and the circumstances under which a payment institution is required to notify a security incident. Those guidelines shall be issued by (insert date - two years of the date of entry into force of this Directive).'</p>

Explanation

Reporting requirements as regards operational and security risks should be defined and assessed by prudential supervisors and central banks. Information can be shared with ENISA or competent authorities under the NIS directive, with the EBA as the appropriate authority for coordination.

Amendment 33

Article 87

<p>'1. Member States shall ensure that a payment service provider applies strong customer authentication when the payer initiates an electronic payment transaction unless EBA guidelines allow specific exemptions based on the risk involved in the provided payment service. This also applies to a third party payment service provider when initiating a payment transaction on behalf of the payer. The account servicing payment service provider shall allow the third party payment service provider to rely on the authentication methods of the former when acting on behalf of the payment service user.</p> <p>2. Where a payment service provider provides services referred to in point 7 of Annex I, it shall authenticate itself towards the account servicing payment service provider of the account owner.'</p>	<p>'1. Member States shall ensure that a payment service provider applies strong customer authentication when the payer initiates an electronic payment transaction unless EBA guidelines allow specific exemptions based on the risk involved in the provided payment service. This also applies to a third party payment service provider when initiating a payment transaction on behalf of the payer. The account servicing payment service provider shall allow the third party payment service provider to rely on the authentication methods of the former when acting on behalf of the payment service user.</p> <p>2. Where a payment service provider provides services referred to in point 7 of Annex I, it shall authenticate itself towards the account servicing payment service provider of the account owner.'</p>
---	---

Explanation

Please see explanation under Amendment 24.

Text proposed by the Commission	Amendments proposed by the ECB ⁽¹⁾
Amendment 34	
Article 89(5) (new)	
No text	<p>'5. EBA shall, in close cooperation with the ECB, issue guidelines addressed to the competent authorities in accordance with Article 16 of Regulation (EU) No 1093/2010, on the complaints procedures to be used to ensure compliance with the relevant provisions under this Directive as set out under paragraph 1 above. Those guidelines shall be issued by [insert date - two years from the date of entry into force of this Directive] and be updated on a regular basis as appropriate.'</p>

Explanation

Harmonised procedures for complaints would facilitate the handling of cross-border complaints and contribute to smooth and efficient compliance procedures supporting the competent authorities in their duties under the proposed directive.

- (¹) Bold in the body of the text indicates where the ECB proposes inserting new text. Strikethrough in the body of the text indicates where the ECB proposes deleting text.
- (²) Directive XXXX/XX/EU of the European Parliament and of the Council of [date] concerning measures to ensure a high common level of network and information security across the Union (OJ L x, p x).
- (³) Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p.37).