Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2023/0209 (COD)
2023/0210 (COD)

Brussels, 03 April 2025

WK 4435/2025 INIT

LIMITE

EF
ECOFIN
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

REQUEST FOR CONTRIBUTION

From:	General Secretariat of the Council
To:	Working Party on Financial Services and the Banking Union (Payment Services/ PSR/PSD) Financial Services Attachés
Subject:	Presidency Questionnaire on PSR Rec + Art. 1-48- Table for comments, Ddl 24 March 2025

PUBLIC

Note from the Presidency: The areas in light blue represent the provisions that are still under discussion and analysis - mainly the issues discussed at the Council Working Party meetings in January and February. Written contributions from Member States following these meetings are still being analysed.

Commission proposal	Legacy text of previous Presidencies	PL PRES drafting suggestions	MS drafting suggestions and comments
2023/0210 (COD) **Proposal for a** **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL** **on payment services in the internal market and amending Regulation (EU) No 1093/2010** **(Text with EEA relevance)**	**Proposal for a** **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010, Regulation (EU) No 2021/1230 and Regulation (EU) 2024/886**		
THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,			
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,			
Having regard to the proposal from the European Commission,			

PUBLIC

After transmission of the draft legislative act to the national parliaments,			
Having regard to the opinion of the European Economic and Social Committee[1],			
Having regard to the opinion of the European Central Bank[2],			
Acting in accordance with the ordinary legislative procedure,			
Whereas:			
(1) Since the adoption of Directive (EU) 2015/2366 of the European Parliament and of the Council[3] the retail payment services market underwent significant changes largely related to the increasing use of cards and digital means of payment, the decreasing use of cash and the growing presence of new players and services, including digital wallets and contactless payments. The Covid-19 pandemic and the transformations it brought to consumption and payment practices has			

[1] OJ C , , p. .

[2] OJ C , , p. .

[3] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (OJ L 337, 23.12.2015, p. 35).

PUBLIC

increased the importance of having secure and efficient payments.			
(2) The Communication from the Commission on a Retail Payments Strategy for the EU[4] announced the launch of a comprehensive review of the application and impact of Directive (EU) 2015/2366 "*which should include an overall assessment of whether it is still fit for purpose, taking into account market developments*".			
(3) Directive (EU) 2015/2366 aimed at addressing barriers to new types of payment services and at improving the level of consumer protection and security. The evaluation of the impact and application of Directive (EU) 2015/2366 by the Commission found that Directive (EU) 2015/2366 has been largely successful with regard to many of its objectives, but also identified certain areas where the objectives of that Directive have not been fully achieved. For example, the evaluation identified the rise in new types of fraud as an issue of concern with regard to consumer protection objectives. Shortcomings have			

4 COM/2020/592 final.

PUBLIC

also been identified with regard to the objective of improving competition in the market thanks to the so-called 'open banking services' (account information services and payment initiation services) by lowering market barriers faced by third party providers. Progress towards the objective of improving the provision of cross-border payment services has also been limited, largely due to inconsistencies in supervisory practices and enforcement across the Union. The evaluation also identified factors stifling progress concerning the objective of levelling the playing field between all payment service providers.			
(4) The evaluation also identified problems regarding divergent implementation and enforcement of Directive (EU) 2015/2366 which directly impact competition between payment service providers, by creating different regulatory conditions in different Member States, encouraging regulatory arbitrage. There should be no room for 'forum shopping' where payment services providers would choose, as 'home country', those Member			

PUBLIC

States where the application of Union rules on payment services is more advantageous for them and provide cross-border services in other Member States which apply stricter interpretation of the rules or apply more active enforcement policies to payment service providers established there. That practice distorts competition. The Union rules on payment services should therefore be further harmonised, by incorporating rules governing the conduct of the payment services activity, including the rights and obligations of the parties involved, in a Regulation. Such rules, excluding the rules on authorisation and supervision of payment institutions, which should remain in a Directive, should be clarified and more detailed, thus minimising margins of interpretation.			
(5) Even though the issuance of electronic money is regulated under Directive 2009/110/EC of the European Parliament and of the Council[5] the use of electronic money to fund payment			

[5] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (OJ L 267, 10.10.2009, p. 7).

PUBLIC

transactions is to a very large extent regulated by Directive (EU) 2015/2366. Consequently, the legal framework applicable to electronic money institutions and payment institutions, in particular with regard to the conduct of business rules, is already substantially aligned. To address the external coherence issues and given the fact that electronic money services and payment services are increasingly hard to distinguish, the legislative frameworks concerning electronic money institutions and payment institutions should be brought closer together. However, the licensing requirements, in particular initial capital and own funds, and some key basic concepts governing the electronic money business such as issuance of electronic money, electronic money distribution and redeemability, are distinct from the services provided by payment institutions. It is therefore appropriate to preserve these specificities when merging the provisions of Directive (EU) 2015/2366 and Directive 2009/110/EC. Since Directive 2009/110/EC is repealed by Directive (EU) XXXX [PSD3], its rules, except for the rules on authorisation and supervision, which have			

PUBLIC

been incorporated in Directive (EU) XXX [PSD3], should be brought into a unified framework under this Regulation, with appropriate adjustments.			
(6) To ensure legal certainty and a clear scope of application of the rules applicable to the conduct of business of providing payment and electronic money services, it is necessary to specify the categories of payment service providers which are subject to the obligations concerning the conduct of the business of providing payment services and electronic money services throughout the Union.			
(7) There are several categories of payment service providers. Credit institutions take deposits from users that can be used to execute payment transactions. They are authorised pursuant to Directive 2013/36/EU of the European Parliament and of the Council[6]. Payment institutions don't take deposits. They may hold users funds and issue electronic money that can be used to execute payment transactions. They are authorised pursuant to Directive (EU) XXX [PSD3]. Post office giro institutions which are entitled to do so under national law may		(7) There are several categories of payment service providers. Credit institutions take deposits from users that can be used to execute payment transactions. They are authorised pursuant to Directive 2013/36/EU of the European Parliament and of	

PUBLIC

also provide electronic money and payment services. Other categories of payment service providers include the European Central Bank (ECB) and national central banks when not acting in their capacity as monetary authority or other public authorities, and Member States or their regional or local authorities when not acting in their capacity as public authorities.		the Council[6]. Payment institutions are not allowed to ~~don't~~ take deposits. They may hold users funds and issue electronic money that can be used to execute payment transactions. They are authorised pursuant to Directive (EU) XXX [PSD3]. Post office giro institutions which are entitled to do so under national law may also provide electronic money and payment services. Other categories of payment service providers include the European Central Bank (ECB) and national central banks when not acting in their capacity as monetary authority or other public authorities, and Member States or their regional or	

[6] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC Text with EEA relevance (OJ L 176, 27.6.2013, p. 338).

		local authorities when not acting in their capacity as public authorities. *[**PRES comment:** Technical amendment based on the Member State's comment.]*	
(8) It is appropriate to dissociate the service of enabling cash to be withdrawn from a payment account from the activity of servicing a payment account, as the providers of cash withdrawal services may not service payment accounts. The services of issuing payment instruments and of acquiring payment transactions, which were listed together in point 5 of the Annex to Directive (EU) 2015/2366 as if one could not be offered without the other, should be presented as two different payment services. Listing issuing and acquiring services separately should, together with distinct definitions of each service, clarify that the issuing and acquiring services may be offered separately by payment service providers.			
(9) The exclusion from the scope of Directive (EU) 2015/2366 of certain			

PUBLIC

categories of operators of automated teller machines (ATM) has proven difficult to apply in practice. Therefore, the category of ATM operators which were excluded from the requirement to be authorised as a payment service provider under Directive (EU) 2015/2366 should be replaced by a new category of ATM operators which do not service payment accounts. While those operators are not subject to the authorisation requirements under Directive (EU) XXX [PSD3], they should however be subject to requirements on fees transparency in situations where such ATM operators levy charges for cash withdrawals.			
(10) To further improve access to cash, which is a priority of the Commission, merchants should be allowed to offer, in physical shops, cash provision services even in the absence of a purchase by a customer, without having to obtain a payment service provider authorisation or being an agent of a payment institution. Those cash provision services should, however, be subject to the obligation to disclose fees charged to the customer, if any. These services should be			

PUBLIC

provided by retailers on a voluntary basis and should depend on the availability of cash by the retailer.			
(11) The exclusion from the scope of Directive (EU) 2015/2366 of payment transactions from the payer to the payee through a commercial agent acting on behalf of the payer or the payee has been applied very differently across Member States. The concept of commercial agents is typically defined in national civil law, which might diverge form Member State to Member State, leading to inconsistent treatment of the same services in different jurisdictions. The concept of commercial agents under that exclusion should therefore be harmonised and clarified by making reference to the definition of commercial agents as laid down in Council Directive 86/653/EEC[7]. In addition, further clarity should be provided on the conditions under which payment transactions from the payer to the payee through commercial agents may be excluded from the scope of this Regulation. This is		(11) The exclusion from the scope of Directive (EU) 2015/2366 of payment transactions from the payer to the payee through a commercial agent acting on behalf of the payer or the payee has been applied very differently across Member States. The concept of commercial agents is typically defined in national civil law, which might diverge from ~~form~~ Member State to Member State, leading to inconsistent treatment of the same services in different jurisdictions. The concept of commercial agents under that exclusion should therefore be	

[7] Council Directive 86/653/EEC of 18 December 1986 on the coordination of the laws of the Member States relating to self-employed commercial agents (OJ L 382, 31.12.1986, p. 17–21).

PUBLIC

achieved by requiring that agents should be authorised via an agreement with either the payer or the payee to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee, but not both of them, regardless of whether or not the commercial agent is in the possession of client's funds. Electronic commerce platforms that act as commercial agents on behalf of both individual buyers and sellers without buyers or sellers having any real margin or autonomy to negotiate or to conclude the sale or purchase of goods or services should not be excluded from the scope of this Regulation. The European Banking Authority (EBA) should develop guidelines on the exclusion for payment transactions from the payer to the payee through a commercial agent to provide further clarity and convergence among competent authorities. Those guidelines may include a repository of use cases typically covered by the commercial agent exclusion.		harmonised ~~and clarified by making reference to the definition of commercial agents as laid down in Council Directive 86/653/EEC[7]~~. In addition, further clarity should be provided on the conditions under which payment transactions from the payer to the payee through commercial agents may be excluded from the scope of this Regulation. This is achieved by requiring that agents should be authorised via an agreement with either the payer or the payee to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee, but not both of them~~, regardless of whether or not the commercial agent is in the possession of client's funds~~. Electronic commerce	

PUBLIC

		platforms that act as commercial agents on behalf of both individual buyers and sellers without buyers or sellers having any real scope ~~margin~~ or autonomy to negotiate or to conclude the sale or purchase of goods or services should not be excluded from the scope of this Regulation. The European Banking Authority (EBA) should develop guidelines on the exclusion for payment transactions from the payer to the payee through a commercial agent to provide further clarity and convergence among competent authorities. Those guidelines may include a repository of use cases typically covered by the commercial agent exclusion. ***[PRES comment:*** *The amendment follows the changes to Article 2(2)(b)*	

PUBLIC

		made by previous Presidencies.]	
(12) The exclusion from the scope of Directive (EU) 2015/2366 related to specific-purpose instruments has been applied differently across Member States, although service providers whose instruments were covered by that exclusion were required to notify their activity to the competent authorities. The EBA provided further guidance in its '*Guidelines on the limited network exclusion under PSD2'* of 24 February 2022[8]. Despite these attempts to clarify the application of the exclusion related to specific-purpose instruments there are still service providers that provide services which involve substantial payment volumes and a variety of products offered to a large number of customers that seek to make use of that exclusion. In these cases, consumers do not benefit from the necessary safeguards and the services should not benefit from the exclusion for specific-purpose instruments. Therefore, it is necessary to clarify that it should not be			

[8] European Banking Authority, EBA/GL/2022/02.

PUBLIC

possible to use the same specific-purpose instrument to make payment transactions to acquire goods and services within more than one limited network or to acquire an unlimited range of goods and services.			
(13) To assess whether a limited network should be excluded from scope, the geographical location of the points of acceptance of such network as well as the number of the points of acceptance should be considered. Specific-purpose instruments should allow the holder to acquire goods or services only in the physical premises of the issuer, whereas usage in an online store environment should not be covered by the notion of premises of the issuer. Specific-purpose instruments should include, depending on the respective contractual regime, cards that can only be used in a particular chain of stores or a particular shopping centre, fuel cards, membership cards, public transport cards, parking ticketing, meal vouchers or vouchers for specific services, which may be subject to a specific tax or labour legal framework designed to promote the use of such		(13) To assess whether a limited network should be excluded from scope, ~~the geographical location of the points of acceptance of such network as well as~~ the number of the points of acceptance should be considered. Specific-purpose instruments should allow the holder to acquire goods or services only in the physical premises of the issuer, whereas usage in an online store environment should not be covered by the notion of premises of the issuer. Specific-purpose instruments should include, depending on the respective contractual regime, cards that can only be	

PUBLIC

instruments to meet the objectives laid down in social legislation, such as childcare vouchers or ecological vouchers. Specific-purpose instruments should also include electronic money-based instruments once they meet the requirements of this exclusion. Payment instruments which can be used for purchases in stores of listed merchants should not be excluded, as such instruments are typically designed for a network of service providers which is continuously growing.		used in a particular chain of stores or a particular shopping centre, fuel cards, membership cards, public transport cards, parking ticketing, meal vouchers or vouchers for specific services, which may be subject to a specific tax or labour legal framework designed to promote the use of such instruments to meet the objectives laid down in social legislation, such as childcare vouchers or ecological vouchers. Specific-purpose instruments should also include electronic money-based instruments once they meet the requirements of this exclusion. Payment instruments which can be used for purchases in stores of listed merchants should not be excluded, as such instruments are typically	

		designed for a network of service providers which is continuously growing. ***[PRES comment:*** *Based on the proposal of one of the Member States that argue whether that in EU, where single market is adopted, the geographical location could be a decisive criterion. The services in EU are provided on cross-border basis. Thus, it seems as it cannot be said that some activity is not covered by limited network exemption only due to the fact that it is provided in more than one Member State.]*	
(14) The exclusion relating to certain payment transactions by means of telecom or information technology devices should focus specifically on micro-payments for digital content and voice-based services. A clear reference to payment transactions for the purchase of electronic tickets should be kept	(14) The exclusion relating to certain payment transactions by means of telecom or information technology devices should focus specifically on micro-payments for digital content and voice-based services. A clear reference to payment transactions for		

PUBLIC

to so that customers can still easily order, pay for, obtain and validate electronic tickets from any location and at any time using mobile phones or other devices. Electronic tickets allow and facilitate the delivery of services that consumers could otherwise purchase in paper ticket form and include transport, entertainment, car parking and entry to venues, but exclude physical goods. Payment transactions by a specified provider of electronic communications networks performed from or via an electronic device and charged to the related bill to collect charitable donations should also be excluded. It should apply only where the value of payment transactions is below a specified threshold.	the purchase of electronic tickets should be kept to so that customers can still easily order, pay for, obtain and validate electronic tickets from any location and at any time using mobile phones or other devices. Electronic tickets allow and facilitate the delivery of services that consumers could otherwise purchase in paper ticket form and include transport, entertainment, car parking and entry to venues, but exclude physical goods. Payment transactions by a specified provider of electronic communications networks performed from or via an electronic device and charged to the related bill to collect charitable donations should also be excluded. It should apply only where the value of payment transactions is below a specified threshold. <u>For the exclusion, the telecommunications operator must provide the payment services in addition to the electronic communications services it provides to its subscriber. This implies that there is a direct contractual</u>		

PUBLIC

	arrangement between the telecommunications operator and the subscriber for the provision of the electronic communications services and that the payment sevice is an additional service to these services. There are situations in which a digital content provider or the provider of services, for which the subscriber has paid through its own telecommunication operator, makes use of further service providers ('intermediaries') for the collection and transfer of the funds. Although those intermediaries (beneficiary operators, collection operators, transit operators etc.) may also provide telecommunication services, cannot benefit from the exclusion, as they do not have a direct contractual relationship with the subscriber regarding the provision of telecommunication services.		
(15) The Single Euro Payments Area (SEPA) has facilitated the creation of Union wide 'payment factories' and 'collection			

PUBLIC

factories', allowing for the centralisation of payment transactions of the same group. In that respect, payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking which are provided by a payment service provider belonging to the same group should be excluded from the scope of this Regulation. The collection of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission to another payment service provider should not be considered as a payment service.			
(16) The provision of payment services requires the support of technical services. Those technical services include the processing and storage of data, payment gateway services, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of consumer-facing interfaces used to collect payment information, including terminals and devices used for payment services. Payment		(16) The provision of payment services requires the support of technical services. Those technical services include the processing and storage of data, payment gateway services, trust and privacy protection services, data and entity authentication, information and communication technology (ICT) and	

PUBLIC

initiation services and account information services are not technical services.		communication network provision, provision and maintenance of consumer-facing interfaces used to collect payment information, including terminals and devices used for payment services. Payment initiation services and account information services are not technical services. ***[PRES comment:*** *Technical amendment.]*	
(17) Technical services do not constitute payment services as such as technical service providers do not enter at any time into possession of the funds to be transferred. They should therefore be excluded from the definition of payment services. Those services should however be subject to certain requirements, such as those on liability for failure to support the application of strong customer authentication, or the requirement to enter into outsourcing agreements with payment service providers in case technical service providers are to provide and verify			

PUBLIC

the elements of strong customer authentication. There should also be requirements governing the termination fees of framework contracts where payment services are offered jointly with technical services.			
(18) Taking into account the rapid evolution of the retail payments market and the emergence of new payment services and payment solutions, it is appropriate to adapt some of the definitions under Directive (EU) 2015/2366 to the realities of the market in order to ensure that Union legislation remains fit for purpose and technology neutral.			
(19) The clarification of the process and the various steps to be followed for the execution of a payment transaction is of significant importance for the rights and obligations of the parties involved in a payment transaction and for the application of strong customer authentication. The process leading to the execution of a payment transaction is either initiated by the payer or on his/her behalf, or by the payee. The payer initiates the payment transaction by placing a			

PUBLIC

payment order. Once the payment order is placed, the payment service provider checks if the transaction has been authorised and authenticated including, where applicable, by applying strong customer authentication, and the payment service provider then validates the payment order. The payment service provider then takes the relevant steps to execute the payment transaction, including the transfer of funds.			
(20) Given the diverging views identified by the Commission in it its review of the implementation of Directive (EU) 2015/2366 and highlighted by the European Banking Authority (EBA) in its opinion of 23 June 2022 on the review of Directive (EU) 2015/2366, it is necessary to clarify the definition of a payment accounts. The determining criterion for the categorisation of an account as payment account lies in the ability to perform daily payment transactions from such an account. The possibility of making payment transactions to a third party from an account or of benefiting from such transactions carried out by a third party is a defining	(20) Given the diverging views identified by the Commission in it its review of the implementation of Directive (EU) 2015/2366 and highlighted by the European Banking Authority (EBA) in its opinion of 23 June 2022 on the review of Directive (EU) 2015/2366, it is necessary to clarify the definition of a payment accounts. The determining criterion for the categorisation of an account as payment account lies in the ability to perform daily payment transactions from such an account. The possibility of making payment transactions to a third party from an account or of		

PUBLIC

feature of the concept of payment account. A payment account should therefore be defined as an account that is used for sending and receiving funds to and from third parties. Any account that possesses those characteristics should be considered a payment account and should be accessed for the provision of payment initiation and account information services. Situations where another intermediary account is needed to execute payment transactions from or to third parties should not fall under the definition of a payment account. Savings accounts are not used for sending and receiving funds to or from a third party, excluding them therefore from the definition of a payment account.	benefiting from such transactions carried out by a third party is a defining feature of the concept of payment account. A payment account should therefore be defined as an account that ~~is~~ can be used for sending and receiving funds to and from third parties. Any account that possesses those characteristics should be considered a payment account and should be accessed for the provision of payment initiation and account information services. In certain cases, such as that of credit card accounts, a case-by-case analysis should be carried out to determine whether it possesses those characteristics. Situations where another intermediary account is needed to execute payment transactions from or to third parties should not fall under the definition of a payment account. Savings accounts that cannot be ~~are not~~ used for sending and receiving funds to or from a third party~~, excluding them therefore~~ are		

PUBLIC

	therefore excluded from the definition of a payment account.		
(21) Given the emergence of new types of payment instruments and the uncertainties prevailing in the market as to their legal qualification, the definition of a 'payment instrument' should be further specified by providing some examples to illustrate what constitutes or does not constitute a payment instrument, bearing in mind the principle of technology neutrality.			
(22) Despite the fact that Near-Field Communication (NFC) enables the initiation of a payment transaction, considering it as a fully-fledged 'payment instrument' would pose some challenges, for example for the application of strong customer authentication for contactless payments at the point of sale and of the payment service provider's liability regime. NFC should therefore rather be considered as a functionality of a payment instrument and not as a payment instrument as such.			
(23) The definition of 'payment instrument' under Directive (EU) 2015/2366 referred to a 'personalised device'. Since			

PUBLIC

there are pre-paid cards where the name of the holder of the instrument is not printed on the card, applying that reference could leave those types of cards outside the scope of the definition of a payment instrument. The definition of 'payment instrument' should, therefore, be amended to refer to 'individualised' devices instead of 'personalised' ones, clarifying that pre-paid cards where the name of the holder of the instrument is not printed on the card fall within the scope of this Regulation.			
(24) So-called digital 'pass-through wallets', involving the tokenisation of an existing payment instrument, for example a payment card, are to be considered as technical services and should thus be excluded from the definition of payment instrument as, in the Commission's view, a token cannot be regarded as being itself a payment instrument but, rather, a 'payment application' within the meaning of Article 2(21) of Regulation (EU) 2015/751 of the European Parliament and of the Council.[9] However, some other categories of digital wallets, namely pre-paid electronic wallets		(24) So-called digital 'pass-through wallets', involving the tokenisation of an existing payment instrument, for example a payment card, are to be considered as technical services and should thus be excluded from the definition of payment instrument as, in the Commission's view, a token cannot be regarded as being itself a payment instrument but, rather, a	

PUBLIC

such as 'staged-wallets' where users can store money for future online transactions, should be considered a payment instrument and their issuance a payment service.		'payment application' within the meaning of Article 2(21) of Regulation (EU) 2015/751 of the European Parliament and of the Council.[9] However, some other categories of digital wallets, namely pre-funded ~~paid~~ electronic wallets such as 'staged-wallets' (characterised by a funding-stage and a payment-stage) where users can store money for future ~~online~~ transactions or where users can fund the wallet simultaneously as it is used, should be considered a payment instrument and their issuance a payment service. ***[PRES comment:*** *Based on the comment of one of the Member States that suggests to clarify that digital staged wallets, which can be funded*	

[9] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (OJ L 123, 19.5.2015, p. 1).

		simultaneously with a purchase by means of a e.g. card payment or credit transfer, but perhaps do not support that users can store money as such within the wallet is also to be considered a payment instrument. There are digital staged wallets operating with this kind of business model (without being a pass-through wallet) in the market but the recital only mentions digital staged wallets where money can be stored.]	
(25) Technological developments since the adoption of Directive (EU) 2015/2366 have transformed the way account information services are provided. The companies offering those services provide payment service users with aggregated online information on one or more of their payment accounts held with one or more payment service providers and accessed via online interfaces of the account servicing			

PUBLIC

payment service provider. Payment service users are thus able to have an overall and structured view of their payment accounts immediately and at any given moment.			
(26) The Commission's review highlighted the fact that authorised account information service providers sometimes provide payment account data that they have aggregated not to the consumer from which they received their permission to access and aggregate the data, but to another party, to enable it to provide other services to the consumer using the data. There are however diverging views as to whether this activity falls under the regulated account information service. The Commission considers that this 'license-as-a-service' evolution of the 'open banking' business model can be a source of innovative, data-based services, to the ultimate benefit of end-users. Indeed, that business model enables end-users to give access to their payment account data in order to receive other - non-payment - services including lending, accounting, creditworthiness assessment. It is however essential that payment service users know			

PUBLIC

precisely who accesses their payment account data, on what legal grounds and for what purpose. Payment service users should be made fully aware of and authorise the transmission of their data to another company. That new open banking-based business model requires a modification of the definition of account information services, to clarify that the information aggregated by the authorised account information service provider may be transmitted to a third party to enable that third party to provide another service to the end-user, with the end-user's permission. To provide consumers with adequate protection for their payment account data and legal certainty about the status of entities accessing their data, the service of data aggregation from payment accounts should always be provided by a regulated entity on the basis of a license, even where the data is ultimately transmitted to another service provider.			
(27) Money remittance is a payment service that is usually based on cash provided by a payer to a payment service provider, without any payment accounts being created			

PUBLIC

in the name of the payer or the payee, which remits the corresponding amount to a payee or to another payment service provider acting on behalf of the payee. In some Member States, supermarkets, merchants and other retailers provide to the public a service enabling the public to pay utilities and other regular household bills. Those bill-paying services should be treated as money remittance.			
(28) The definition of funds should cover all forms of central bank money issued for retail use, including banknotes and coins, and any possible future central bank digital currency, e-money and commercial bank money. Central bank money issued for use between the central bank and commercial banks, i.e. for wholesale use, should not be covered.			
(29) Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets lays down that electronic-money tokens shall be deemed to be electronic money. Electronic money tokens are therefore included, as electronic money, in the definition of funds in this Regulation.	(29) Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets lays down that electronic-money tokens shall be deemed to be electronic money. Electronic money tokens are therefore included, as electronic money, in the definition of	(29) Regulation (EU) 2023/1114 ~~of 31 May 2023 on markets in crypto-assets~~ lays down that electronic-money tokens shall be deemed to be electronic money. Accordingly,	

	funds in this Regulation. Likewise, the requirements of this Regulation should apply to crypto-asset services, as defined in Regulation (EU) 2023/1114 of 31 May 2023, provided in relation to, or with, electronic money tokens, where such services are payment services.	references to electronic money in this Regulation should be understood to include electronic money tokens, unless otherwise stated, and ~~E~~electronic money tokens ~~are therefore~~ should be included, as electronic money, in the definition of funds ~~in this Regulation~~. Likewise, the requirements of this Regulation should apply to crypto-asset service~~s~~ providers, ~~as defined in Regulation (EU) 2023/1114 of 31 May 2023,~~ providing crypto-asset services ~~in relation to, or~~ with~~,~~ electronic money tokens, where such services are payment services. This concerns in particular transfers by crypto-asset service providers, on behalf of their clients, of electronic money tokens corresponding to	

		transfer services for crypto-assets on behalf of clients under Regulation 2023/1114. Such services could qualify as the payment service of executing payment transactions, for example, where a crypto-asset service provider offers custodial wallets enabling transfers on behalf of its clients of electronic money tokens to and from third parties, or to other accounts of its clients. *[**PRES comment:** Proposal from the February CWP meeting.]*	
		(29a) Given the market evolution since the adoption of Directive (EU) 2015/2366, and in order to avoid disproportionate requirements for crypto-asset service providers that provide services with electronic money tokens in	

		accordance with Regulation (EU) 2023/1114, and also to ensure legal clarity as regards the scope of application of this Regulation and Directive xx [PSD3] to services with electronic money tokens, it is appropriate to exclude from the scope of application of this Regulation and Directive xx [PSD3] certain types of payment transactions with electronic money tokens where electronic money tokens are used for investment or trading purposes. This concerns in particular the exchange by crypto-asset service providers of electronic money tokens for funds or crypto-assets, regardless of whether the crypto-asset service providers are intermediating between buyers and sellers, or acting in their own name as sellers	

		or buyers of electronic money tokens. This exclusion should cover in particular exchanges of electronic money tokens as part of the provision of the service of exchanging crypto-assets for funds, exchanging crypto-assets for other crypto-assets, operating a trading platform for crypto-assets, receiving and transmitting orders for crypto-assets on behalf of clients or executing orders for crypto-assets on behalf of clients, as defined in Regulation (EU) 2023/1114. However, the exclusion should not include transfer services where electronic money tokens are used to pay for goods or services, for peer-to-peer payment transactions or payment transactions between payment accounts held by the	

		same person. *[**PRES comment:** Proposal from the February CWP meeting.]*	
		(29b) Since Directive (EU) 2015/2366 also included a specific exclusion regarding payment transactions made exclusively in cash directly from the payer to the payee without any intermediary intervention, it is appropriate to include a similar exclusion regarding transactions with electronic money tokens carried out without any intermediary involved. This should include transfers of electronic money tokens between two self-hosted addresses, where there is no intermediary involved, either on the side of the payer or on the side of the payee, and should not include payment transactions between a	

		custodial wallet and a self-hosted wallet. *[**PRES comment:** Proposal from the February CWP meeting.]*	
(30) To preserve the confidence of the electronic money holder, electronic money needs to be redeemable. Redeemability does not imply that the funds received in exchange for electronic money should be regarded as deposits or other repayable funds for the purpose of Directive 2013/36/EU[10]. Redemption should be possible at any time, at par value, without any possibility to agree on a minimum threshold for redemption. Redemption should, in general, be granted free of charge. However, it should be possible to request a proportionate and cost-based fee, without prejudice to national legislation on tax or social matters or any obligations on the electronic money issuer under other relevant Union or national legislation, including anti-money laundering and anti-terrorist financing rules, to any			

[10] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338–436).

PUBLIC

action targeting the freezing of funds or any specific measure linked to the prevention and investigation of crimes.			
(31) Payment service providers need access to payment systems to provide payment services to users. Those payment systems typically include four-party card schemes as well as major systems processing credit transfers and direct debits. To ensure equality of treatment throughout the Union between the different categories of authorised payment service providers it is necessary to clarify the rules concerning access to payment systems. Such access may be direct or indirect via another participant in that payment system. Such access should be subject to requirements that ensure integrity and stability of those payment systems. To that end the payment system operator should carry out a risk assessment of a payment service provider which applies for direct participation; that risk assessment should examine all relevant risks, including where applicable settlement risk, operational risk, credit risk, liquidity risk and business risk. Each payment service provider applying for			

PUBLIC

participation in a payment system should bear the risk of its own choice of system and provide proof to the payment system that its internal arrangements are sufficiently robust against those types of risk. Payment system operators should only reject an application for direct participation by a payment service provider if the payment service provider is unable to respect the rules of the system or poses an unacceptably high level of risk.			
(32) Payment system operators should have in place rules and procedures on access which are proportionate objective non-discriminatory and transparent. Payment system operators should not discriminate against payment institutions as regards participation if the system rules can be respected and there is no unacceptable risk to the system. Such systems include, amongst others, those designated under Directive 98/26/EC of the European Parliament and of the Council[11]. In cases where the payment system in question is already subject to			

[11] Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems (OJ L 166, 11.6.1998, p. 45).

PUBLIC

oversight by the European System of Central Banks under Regulation of the European Central Bank (EU) No 795/2014[12], the central bank or banks exercising that oversight should monitor respect of those rules in the framework of their oversight. In cases of other payment systems, Member States should designate national competent authorities to ensure that payment system infrastructure operators respect such requirements.			
(33) To ensure fair competition between payment service providers, a participant in a payment system which provides services in relation to such a system to an authorised or registered payment service provider should also, when requested to do so, grant access to such services in an objective, proportionate and non-discriminatory manner to any other authorised or registered payment service provider.			
(34) The provisions relating to access to payment systems should not apply to systems set up and operated by a single payment			

[12] Regulation of the European Central Bank (EU) No 795/2014 of 3 July 2014 on oversight requirements for systemically important payment systems (OJ L 217, 23.7.2014, p. 16).

PUBLIC

service provider. Such payment systems can operate either in direct competition to other payment systems or, more typically, in a market niche not covered by other payment systems. Such systems include three-party schemes, including three-party card schemes, to the extent that those schemes never operate as de facto four-party card schemes, including by relying upon licensees, agents or co-branding partners. Such systems also typically include payment services offered by telecommunication providers where the scheme operator is the payment service provider both to the payer and to the payee, and internal systems of banking groups. To stimulate the competition that can be provided by such closed payment systems to established mainstream payment systems, access to those closed proprietary payment systems should not be granted to third parties. However, such closed systems should always be subject to Union and national competition rules which may require that access be granted to the schemes in order to maintain effective competition in payments markets.			

PUBLIC

(35) Payment institutions need to be able to open and maintain an account with a credit institution to meet their licensing requirements as regards safeguarding of customer funds. However, as evidenced in particular by the EBA in its Opinion of 5 January 2022,[13] despite the provisions on payment institution accounts with a commercial bank laid down in Directive (EU) 2015/2366, some payment institutions or companies applying for a payment institution license still face practices from some credit institutions which either refuse to open an account for them or close an account where one exists, based on perceived higher risk of money laundering or terrorism financing. Those so-called 'de-risking' practices create significant competitive challenges for payment institutions.			
(36) Credit institutions should therefore provide a payment account to payment institutions, and to applicants for a license as a payment institution, as well as to their agents and distributors, except in exceptional cases where there are serious grounds to	(36) Credit institutions should therefore provide a payment account to payment institutions, and to applicants for a license as a payment institution, as well as to their agents ~~and distributors~~, except in	(36) Credit institutions should therefore provide a payment account based on objective, non-discriminatory and proportionate terms to	

[13] European Banking Authority, EBA/Op/2022/01.

refuse access. It is necessary to include applicants for a license as a payment institution in that provision, given the fact that a bank account where clients' funds can be safeguarded is a prerequisite to obtain a payment institution license. The grounds for refusal should include serious grounds for suspicion of illegal activities being pursued by or via the payment institution, or a business model or risk profile which causes serious risks or excessive compliance costs for the credit institution. For instance, business models where payment institutions use a vast network of agents may generate significant anti-money laundering and combating the financing of terrorism (AML/CFT) compliance costs. A payment institution should have the right of appeal against a refusal by a credit institution to a competent authority designated by a Member State. In order to facilitate the exercise of that appeal right, credit institutions should motivate in writing and in detail any refusal to provide an account, or a subsequent closure of an account. That motivation should refer to specific elements relating to the payment institution in question, not to	exceptional cases where there are serious grounds to refuse access. It is necessary to include applicants for a license as a payment institution in that provision, given the fact that a bank account where clients' funds can be safeguarded is a prerequisite to obtain a payment institution license. ~~The grounds for refusal should include serious grounds for suspicion of illegal activities being pursued by or via the payment institution, or a business model or risk profile which causes serious risks or excessive compliance costs for the credit institution. For instance, business models where payment institutions use a vast network of agents may generate significant anti-money laundering and combating the financing of terrorism (AML/CFT) compliance costs.~~ Credit institutions should not be required to provide or continue providing the services of a payment account to a payment institution or its agents, where this would result in	payment institutions, and to applicants for a license as a payment institution, as well as to their agents ~~and distributors~~, except in exceptional cases where there are serious grounds to refuse access. It is necessary to include applicants for a license as a payment institution in that provision, given the fact that a bank account where clients' funds can be safeguarded is a prerequisite to obtain a payment institution license. ~~The grounds for refusal should include serious grounds for suspicion of illegal activities being pursued by or via the payment institution, or a business model or risk profile which causes serious risks or excessive compliance costs for the credit institution. For~~	

general or generic considerations. To facilitate treatment by competent authorities of appeals against account refusal or withdrawal and motivation thereof, the EBA should develop implementing technical standards harmonising the presentation of such motivations.	an infringement of Regulation (EU) of the European Parliament and of the Council[14]. [Article 14(4) of] that Regulation prohibits the provision of services in situations where the credit institution is unable to comply with certain customer due diligence obligations. An infringement of that Regulation may also arise when the policies, controls and procedures adopted for the purposes of mitigating and managing money laundering and terrorist financing risks do not adequately mitigate the risks associated with a specific business relationship. To that end, credit institutions should be able to refuse the provision of a payment account when the money laundering or terrorist financing risks associated with an existing or prospective customer exceed the risks that the credit institution would be able to	~~instance, business models where payment institutions use a vast network of agents may generate significant anti-money laundering and combating the financing of terrorism (AML/CFT) compliance costs.~~ Credit institutions should not be required to provide or continue providing the services of a payment account to a payment institution or its agents, where this would result in an infringement of Regulation (EU) of the European Parliament and of the Council[14]. ~~[Article 14(4) of]~~ ~~t~~That Regulation prohibits the provision of services in situations where the credit institution is unable to	

[14] OP: Please insert in the text the number of the Regulation contained in document 2021/0239(COD) (Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - COM/2021/420 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.

	manage. The credit institution should also be able to refuse in cases where insufficient relevant information or documents have been received from the applicant to open an account. For instance, when a credit institution cannot perform its customer due diligence obligations due to a lack of information or documents. When requesting information or documents the credit institution should take into account the proportionality principle. A payment institution should have the right of appeal against a refusal by a credit institution to a competent authority designated by a Member State. In order to facilitate the exercise of that appeal right, credit institutions should motivate in writing and in detail any refusal to provide an account, or a subsequent closure of an account to the payment institution, its agents or the applicant for a license as a payment institution. That motivation should refer to specific elements relating to the	comply with certain customer due diligence obligations. An infringement of that Regulation may also arise when the policies, controls and procedures adopted for the purposes of mitigating and managing money laundering and terrorist financing risks do not adequately mitigate the risks associated with a specific business relationship. To that end, credit institutions should be able to refuse the provision of a payment account when the money laundering or terrorist financing risks associated with an existing or prospective customer exceed the risks that the credit institution would be able to manage. The credit institution should also be able to refuse in cases where insufficient relevant	

PUBLIC

	payment institution in question, not to general or generic considerations. Where the payment account is refused on grounds that it would infringe provisions of Regulation (EU) of the European Parliament and of the Council[15], the justification provided to the client or applicant should not lead to the explicit or implicit disclosure of information protected under Article 73 of that Regulation. To that effect, credit institutions should not disclose the details of the anti-money laundering reasons for refusal. To facilitate treatment by competent authorities of appeals against account refusal or withdrawal and motivation thereof, the EBA should develop implementing technical standards harmonising the presentation of such motivations. It is necessary that the EBA issues guidelines on the meaning of 'substantive breach of contract'. The closing of the payment account held by the payment institution should be subject to the	information or documents have been received from the applicant to open an account. For instance, when a credit institution cannot perform its customer due diligence obligations due to a lack of information or documents. When requesting information or documents the credit institution should take into account the proportionality principle. A payment institution should have the right of appeal against a refusal by a credit institution to a competent authority designated by a Member State. In order to facilitate the exercise of that appeal right, credit institutions should motivate in writing and in detail any refusal to provide an account, or a subsequent closure of an account to the payment institution, its	

	finalisation of the clients' reimbursements. The clients' funds should be disbursed before the closing of the account.	agents or the applicant for a license as a payment institution. That motivation should refer to specific elements relating to the payment institution in question, not to general or generic considerations. Where the payment account is refused on grounds that it would infringe provisions of Regulation (EU) of the European Parliament and of the Council[15], the justification provided to the client or applicant should not lead to the explicit or implicit disclosure of information protected under Article 73 of that Regulation. To that effect, credit institutions should not	

[15] OP: Please insert in the text the number of the Regulation contained in document 2021/0239(COD) (Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - COM/2021/420 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.

PUBLIC

		disclose the details of the anti-money laundering reasons for refusal. To facilitate treatment by competent authorities of appeals against account refusal or withdrawal and motivation thereof, the EBA should develop implementing technical standards harmonising the presentation of such motivations. It is necessary that the EBA issues guidelines on the meaning of 'substantive breach of contract'. The closing of the payment account held by the payment institution should be subject to the finalisation of the clients' reimbursements. The clients' funds should be disbursed before the closing of the account. ***[PRES comment:*** *Amendment based on the*	

PUBLIC

		comment of one of the Member States to align the wording to Article 32 PSR.]	
	(36a) The closing of the payment account held by the payment institution should be subject to the finalisation of the clients' reimbursements. The clients' funds should be disbursed before the closing of the account.		
	(36b) The credit institution should each year report information ~~on~~ concerning ~~the closure or refusal to open a~~ payment accounts to a payment institution, its agents or an applicant for a license as a payment institution to the competent authority. This report should contain information on the number of payment accounts opened, the number of refusals and closures of payment accounts and the ground of refusal or closure.		
(37) To make well-informed choices and to be able to choose their payment service provider easily within the Union, payment		(37) To make well-informed choices and to be able to choose their payment	

PUBLIC

service users should receive comparable and clear information about payment services. To ensure that necessary, sufficient and comprehensible information is given to payment service users with regard to the payment service contract and payment transactions, it is necessary to specify and to harmonise the obligations on payment service providers as regards the provision of information to payment service users.		service provider easily within the Union, payment service users should receive comparable ~~and clear~~ information about payment services in a clear, neutral and comprehensible manner. To ensure that necessary, sufficient and comprehensible information is given to payment service users with regard to the payment service contract and payment transactions, it is necessary to specify and to harmonise the obligations on payment service providers as regards the provision of information to payment service users. ***[PRES comment**: Amendment based on the comment of one of the Member States suggesting to introduce a uniform wording as regards the information duties in PSR.]*	

PUBLIC

(38) When providing the required information to payment service users, payment service providers should take into account the needs of payment service users and practical aspects and cost-efficiency depending on the respective payment service contract. Payment service providers should either actively communicate at the appropriate time without any prompting by the payment service user, or they should make the information available to payment service users request. In the second situation, payment service users should take active steps to obtain the information, including requesting that information explicitly from payment service providers, logging into a bank account mailbox or inserting a bank card into a printer for account statements. For those purposes, the payment service providers should ensure that access to the information is possible, and that the information is available to payment service users.			
(39) As consumers and undertakings are not in the same position of vulnerability, they do not need the same level of protection.			

PUBLIC

While it is important to guarantee consumer rights by provisions from which it is not possible to derogate by contract, it is reasonable to let undertakings and organisations agree otherwise when they are not dealing with consumers. Micro-enterprises, as defined in Commission Recommendation 2003/361/EC,[16] may be treated in the same way as consumers. Certain rules should always apply, irrespective of the status of the user.			
	(39a) Independent ATM deployers should display to their customers in a clear, neutral and comprehensible manner, information on any charges before the customer carries out the withdrawal for example by displaying their charges digitally on the terminal. When the transaction is completed, the information on charges should be documented, at the simple request of the customer, on a receipt or another durable medium.	(39a) ~~Independent~~ ATM deployers should display to their customers in a clear, neutral and comprehensible manner, information on any charges before the customer carries out the withdrawal for example by displaying their charges digitally on the terminal. When the transaction is completed, the information on charges should be	

[16] OJ L 124, 20.05.2003, p. 36-41.

PUBLIC

		documented, at the simple request of the customer, on a receipt or another durable medium. ***[PRES comment:*** *Based on the view expressed by a majority of Member States.]*	
(40) To maintain a high level of consumer protection, consumers should have the right to receive information on services conditions and prices free of charge before being bound by any payment service contract. To enable consumers to compare the services and conditions offered by payment service providers and, in the case of a dispute, to verify their contractual rights and obligations, consumers should be able to request that information and the framework contract on paper, free of charge and at any time during the contractual relationship.			
(41) To increase the level of transparency, payment service providers should provide basic information on executed payment transactions at no additional charge to the consumer. In the case of a single payment			

PUBLIC

transaction, the payment service provider should not charge separately for that information. Similarly, payment service providers should provide free of charge and on a monthly basis subsequent information on payment transactions under a framework contract. However, considering the importance of transparency in pricing and differing customer needs, the parties to the contract should be able to agree on charges for more frequent or additional information.			
(42) Low-value payment instruments should be a cheap and easy-to-use alternative in the case of low-priced goods and services and should not be overburdened by excessive requirements. The relevant information requirements and rules on their execution should therefore be limited to essential information, also considering the technical capabilities that can justifiably be expected from instruments dedicated to low-value payments. Despite the lighter regime, payment service users should have adequate protection, having regard to the limited risks posed by those payment instruments, in			

PUBLIC

particular as concerns prepaid payment instruments.			
(43) In single payment transactions, the essential information should always be given at the payment service providers' own initiative. As payers are usually present when giving the payment order, it should not be necessary that information be always provided on paper or on another durable medium. Payment service providers should be able to give information orally or make it otherwise easily accessible, including by keeping the conditions on a notice board on the premises. Information should also be given on where to find other, more detailed, information, including on the website. However, where the consumer so requests, the essential information should also be given by payment service providers on paper or on another durable medium.			
(44) The information required should be proportionate to the needs of users. The information requirements for a single payment transaction should be different from the information requirements for a			

PUBLIC

framework contract which provides for a series of payment transactions.			
(45) To be able to make an informed choice payment service users should be able to compare Automatic Teller Machine (ATM) charges with those of other providers. To increase the transparency of ATM charges for the payment service user payment service providers should provide payment service users with information on all applicable charges for domestic ATM withdrawals in different situations, depending on the ATM from which the payment service users withdraw cash.			
(46) Framework contracts and the payment transactions covered by those contracts are more common and economically significant than single payment transactions. If there is a payment account or a specific payment instrument, a framework contract is required. Therefore, the requirements for prior information on framework contracts should be comprehensive and information should always be provided on paper or on another durable medium. However, payment service			

PUBLIC

providers and payment service users should be able to agree in the framework contract on the manner in which subsequent information on executed payment transactions is to be given.			
(47) Contractual provisions should not discriminate against consumers who are legally resident in the Union on the grounds of their nationality or place of residence. Where a framework contract provides for the right to block a payment instrument for objectively justified reasons, the payment service provider should not be able to invoke that right merely because the payment service user has changed his or her place of residence within the Union.			
(48) To ensure a high level of consumer protection, Member States should, in the interest of the consumer, be able to maintain or introduce restrictions or prohibitions on unilateral changes in the conditions of a framework contract, for instance if there is no justified reason for such a change.	(48) To ensure a high level of consumer protection, Member States should, in the interest of the consumer, be able to maintain or introduce restrictions or prohibitions on unilateral changes in the conditions of a framework contract, for instance if there is no justified reason for such a change. <u>This is without prejudice to Council</u>		

PUBLIC

	Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.		
(49) To facilitate payment service users' mobility, users should be able to terminate a framework contract without incurring charges. However, for contracts terminated by the payment service users less than 6 months after their entry into force, payment service providers should be allowed to apply charges in line with the costs incurred due to the termination of the framework contract by the user. Where, under a framework contract, payment services are offered jointly with technical services supporting the provision of payment services, such as the rental of terminals used for payment services, payment service users should not be locked in with their payment service provider via more onerous terms set in the contractual clauses governing the technical services. To preserve competition, such contractual terms should be subject to the framework contract requirements on termination fees. For consumers, the period of notice agreed should be no longer than 1 month, and for			

PUBLIC

payment service providers no shorter than 2 months. Those rules should be without prejudice to the payment service provider's obligation to terminate the payment service contract in exceptional circumstances under other relevant Union or national law, such as that on money laundering or financing of terrorism, any action targeting the freezing of funds, or any specific measure linked to the prevention and investigation of crimes.			
(50) To achieve comparability, the estimated currency conversion charges for credit transfers and remittances carried out within the Union and from the Union to a third country should be expressed in the same way, namely as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the European Central Bank (ECB). When reference is made to 'charges' in this Regulation, it should also cover, where applicable, 'currency conversion' charges.	(50) To achieve comparability, the estimated currency conversion charges for credit transfers and remittances carried out within the Union and from the Union to a third country should be expressed in the same way, namely as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the European Central Bank (ECB). If the relevant percentage mark-up is not publicly available at the ECB for non-euro currencies, the latest available applicable foreign exchange reference rate issued by the relevant central bank should be used.	(50) To achieve comparability, the estimated currency conversion charges for credit transfers and remittances carried out within the Union and from the Union to a third country should be expressed in the same way, namely as a monetary amount in the currency of the payer's account and as a percentage mark-up over an aggregated live mid-market benchmark rate that accurately reflects the market. To ensure that the	

	For the sake of clarity the estimated currency conversion charges should also be expressed in a monetary amount in the currency of the payer's account. When reference is made to 'charges' in this Regulation, it should also cover, where applicable, 'currency conversion' charges.	benchmark rate used is reliable and accurately reflects the market, it should be provided by a trusted administrator who meets applicable governance and control requirements, such as the IOSCO Principles for Financial Benchmarks. ~~the latest available euro foreign exchange reference rates issued by the European Central Bank (ECB). If the relevant percentage mark-up is not publicly available at the ECB for non-euro currencies, the latest available applicable foreign exchange reference rate issued by the relevant central bank should be used. For the sake of clarity the estimated currency conversion charges should also be expressed in a monetary amount in the currency of the payer's account.~~ When reference is	

		made to 'charges' in this Regulation, it should also cover, where applicable, 'currency conversion' charges. ***[PRES comment:*** *Amendments based on the PRES proposal presented at the January CWP meeting.]*	
	(50a) The time for the funds of credit transfers and money remittance transactions to be received by the payment service provider of the payee located outside the Union should be an estimation. The payment service provider of the payer should make the payer aware that this is not an exact timing, since this could depend on different factors, sometimes out of control of the payer's payment service provider.		
	(50b) The payment service provider can only provide or make available the name of the payee to the payer if this is possible, which is not the case for money remittances. When		

PUBLIC

	executing a money remittance as a single payment transaction, the payment service provider of the payer is unaware of the name of the payee, unless it is provided by the payer. Therefore, in such cases the payment service provider of the payer should not be required to provide or make available such information to the payer.		
(51) Experience has shown that the sharing of charges between a payer and a payee is the most efficient system since it facilitates the straight-through processing of payments. Provision should therefore be made for charges to be levied directly on the payer and the payee by their respective payment service providers. The amount of any charges levied may also be zero as the rules should not affect the practice whereby a payment service provider does not charge consumers for crediting their accounts. Similarly, depending on the contract terms, a payment service provider may charge only the payee for the use of the payment service, in which case no charges are imposed on the			

PUBLIC

payer. It is possible that the payment systems impose charges by way of a subscription fee. The provisions on the amount transferred or any charges levied have no direct impact on pricing between payment service providers or any intermediaries.			
(52) A surcharge is a charge by merchants to consumers that is added on top of the requested price for goods and services when a certain payment method is used by the consumer. One of the reasons for surcharging is to direct consumers to cheaper or more efficient payment instruments, hence fostering competition between alternative payment methods. Under the regime introduced by Directive (EU) 2015/2366, payees were prevented from requesting charges for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751, i.e. for consumer debit and credit cards issued under four-party card schemes, and for those payment services to which Regulation (EU) No 260/2012 of the			

PUBLIC

European Parliament and of the Council[17] applies, i.e. credit transfer and direct debit transactions denominated in euro within the Union. Member States were allowed under Directive (EU) 2015/2366 to further prohibit or limit the right of the payee to request charges, taking into account the need to encourage competition and promote the use of efficient payment instruments.			
(53) Evidence gathered during the review of Directive (EU) 2015/2366 shows that the current rules on charges are appropriate and had a positive impact. There is no compelling need for further alignment of charging practices between Member States, as the existing surcharging ban already applies to a very large share of payments in the Union. It is estimated that 95% of card payments are subject to the existing surcharging ban. In addition, when a surcharge is applied, it is capped at the actual cost incurred by the merchant. However, in its review of Directive (EU) 2015/2366, the Commission identified different interpretations			

[17] 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).

PUBLIC

concerning the payment instruments covered by the surcharging ban. It is therefore necessary to explicitly extend the surcharging ban to all credit transfers and direct debits and not just to those covered by Regulation (EU) No 260/2012, as was the case under Directive (EU) 2015/2366.			
(54) Account information services and payment initiation services, often collectively known as 'open banking services', are payment services involving access to the data of a payment service user by payment service providers which do not hold the account holder's funds nor service a payment account. Account information services allow the aggregation of a user's data, at the request of the payment service user, with different account servicing payment service providers in one single place. Payment initiation services allow the initiation of a payment from the user's account, such as a credit transfer or a direct debit, in a convenient way for the user and the payee without the use of an instrument such as a payment card.	(54) Account information services and payment initiation services, often collectively known as 'open banking services', are payment services involving access to the data of a payment service user by payment service providers which do not hold the account holder's funds nor service a payment account. Account information service~~s~~ providers provide a service that aims to allow the aggregation of a user's data, at the request of the payment service user, with different account servicing payment service providers in one single place. The account information service provider need not be the one that provides this service to the payment service user. It could also		

PUBLIC

	transmit the payment account data obtained to a third party who in turn would provide such a service of aggregation and/or consolidation, possibly with value added services on top, to the payment service user. Payment initiation services allow the initiation of a payment from the user's account, such as a credit transfer or a direct debit, in a convenient way for the user and the payee without the use of an instrument such as a payment card. A payment initiation service necessitates obtaining the mandate of the payer to access the payment account and is therefore by its nature always provided to the payer and never exclusively to a payee. However, as also acknowledged in the AML Regulation, some payment initiation services also establish a business relationship with the payee and therefore, the definition of payment initiation service reflects that the providers of such services may offer payment initiation services		

PUBLIC

	not only to the payer, but in certain cases, also to the payee.		
(55) Account servicing payment service providers should allow access by account information and payment initiation service providers to payment account data if the payment account can be accessed by the payment service user online and if the payment service user has granted permission for such access. Directive (EU) 2015/2366 was based on the principle of access to payment account data without a need for a contractual relationship between the account servicing payment service provider and the account information and payment initiation service providers, which had the effect that charging for access to data was in practice not possible. Access to data under open banking has been taking place on such a non-contractual basis, and without charging, since the application of Directive (EU) 2015/2366. If regulated data access services were to be subjected to a charge, where there was no charge hitherto, the impact on the continued provision of those services, and therefore on competition and innovation in			

PUBLIC

payment markets, could be very significant. That principle should therefore be maintained. Maintaining that approach is in line with Chapters III and IV of the proposal of a Regulation on harmonised rules on fair access to and use of data (Data Act)[18], in particular Article 9(3) of that proposal on compensation, to which this Regulation is without prejudice. The Commission's proposal for a Regulation on Financial Data Access (FIDA) provides for a possible compensation for data access which will be covered by FIDA. Such regime would thus be different from the one governed by the present Regulation. This difference of treatment is justified by the fact that, unlike for payment account data access, which is regulated by Union law since the entry into force of Directive (EU) 2015/2366, access to other financial data has not yet been subject to Union regulation. There is therefore no risk of disruption as, unlike access to payment account data, this market is emerging and will be regulated for the first time with FIDA.			

[18] Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act). COM/2022/68 final

PUBLIC

(56) Account servicing payment service providers and account information and payment initiation service providers may establish a contractual relationship, including in the context of a multilateral contractual arrangement (e.g. a scheme), with possible compensation, for access to payment account data and provision of open banking services other than those required by this Regulation. An example of such value-added services offered via so-called 'premium' Application Programming Interfaces (APIs) is the possibility to schedule future variable recurring payments. Any compensation for such services would have to be in line with Chapters III and IV of the proposed Data Act after its date of application, in particular as regards its articles 9(1) and 9(2) on compensation. Access by account information and payment initiation service providers to payment account data regulated under this Regulation without a requirement of a contractual relationship, and thus without charging, should always be possible even in cases where a multilateral contractual arrangement (e.g. a scheme) is in place and where the same data is also available as part			

PUBLIC

of the said multilateral contractual arrangement.			
(57) To guarantee a high level of security in data access and exchange, access to payment accounts and the data therein should, barring specific circumstances, be provided to account information and payment initiation service providers via an interface designed and dedicated for 'open banking' purposes, such as an API. To that end, the account servicing payment service provider should set up a secure communication with account information and payment initiation service providers. To avoid any uncertainty as to who is accessing the payment service user's data, the dedicated interface should enable account information and payment initiation service providers to identify themselves to the account servicing payment service provider, and to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user. Account information and payment initiation service providers should as a general rule use the interface dedicated	(57) To guarantee a high level of security in data access and exchange, access to payment accounts and the data therein should~~, barring specific circumstances,~~ be provided to account information and payment initiation service providers via an interface designed and dedicated for 'open banking' purposes, such as an API. To that end, the account servicing payment service provider should set up a secure communication with account information and payment initiation service providers. To avoid any uncertainty as to who is accessing the payment service user's data, the dedicated interface should enable account information and payment initiation service providers to identify themselves to the account servicing payment service provider, and to rely on all the authentication procedures provided by the account servicing	(57) To guarantee a high level of security in data access and exchange, access to payment accounts and the data therein should~~, barring specific circumstances,~~ be provided to account information and payment initiation service providers via an interface designed and dedicated for 'open banking' purposes, such as an API. To that end, the account servicing payment service provider should set up a secure communication with account information and payment initiation service providers. To avoid any uncertainty as to who is accessing the payment service user's data, the dedicated interface should enable account information	

for their access and therefore should not use the customer interface of an account servicing payment service provider for the purpose of data access, except in cases of failure or unavailability of the dedicated interface in the conditions laid down in this Regulation. In such circumstances their business continuity would be endangered by their incapacity to access the data for which they have been granted a permission. It is indispensable that account information and payment initiation service providers be at all times able to access the data indispensable for them to service their clients.	payment service provider to the payment service user. Account information and payment initiation service providers should ~~as a general rule~~ use the interface dedicated for their access and therefore should not use the customer interface of an account servicing payment service provider for the purpose of data access. ~~, except~~ In cases of failure or unplanned unavailability of the dedicated interface ~~in the conditions laid down in this Regulation~~, ~~In such circumstances~~ their business continuity would be endangered by their incapacity to access the data for which they have been granted a permission. It is indispensable that account information and payment initiation service providers be at all times able to access the data indispensable for them to service their clients. Therefore, planned unavailability of the dedicated interface, in order to allow the account servicing payment service providers to update or make changes	and payment initiation service providers to identify themselves to the account servicing payment service provider, and to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user. Account information and payment initiation service providers should ~~as a general rule~~ use the interface dedicated for their access and therefore should not use the customer interface of an account servicing payment service provider for the purpose of data access. ~~, except~~ In cases of failure or unplanned unavailability of the dedicated interface ~~in the conditions laid down in this Regulation~~, ~~In such circumstances~~ their business continuity would be	

	to the dedicated interface, should normally occur between 00:00 and 06:00. The normal procedure of system maintenance foresees the upgrade of the system during the night between midnight and 06:00. However, sometimes very large maintenance procedure could take longer than several hours. The timing referred to is expressed in the local time of the account servicing payment service provider. The account servicing payment service provider should as a rule, except for emergency changes, also duly inform payment service providers making use of the dedicated interface at least one month in advance of any planned unavailability and its duration.	endangered by their incapacity to access the data for which they have been granted a permission. It is essential ~~indispensable~~ that account information and payment initiation service providers be at all times able to access the data indispensable for them to service their clients. Therefore, planned unavailability of the dedicated interface, in order to allow the account servicing payment service providers to update or make changes to the dedicated interface, should normally occur between 00:00 and 06:00. The normal procedure of system maintenance foresees the upgrade of the system during the night between 00:00 ~~midnight~~ and 06:00. However, sometimes very large maintenance	

PUBLIC

		procedure could take longer than several hours. The timing referred to is expressed in the local time of the account servicing payment service provider. The account servicing payment service provider should as a rule, except for emergency changes, also duly inform payment service providers making use of the dedicated interface at least one month in advance of any planned unavailability and its duration. ***[PRES comment:*** *Technical amendments based on the Member States' comments.]*	
(58) To facilitate the smooth use of the dedicated interface, its technical specifications should be adequately documented and a summary be made publicly available by the account servicing payment service provider. To enable the open banking service providers to adequately			

PUBLIC

prepare their future access and to solve any possible technical problems, the account servicing payment service provider should enable account information and payment initiation service providers to test an interface prior to the date on which the interface will be activated. Only authorised account information and payment initiation service providers should access payment account data via that interface, although applicants for authorisation as account information and payment initiation service providers should be able to consult the technical specifications. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international or European standardisation organisations including the European Committee for Standardization (CEN) or the International Organization for Standardization (ISO).			
(59) For account information and payment initiation service providers to ensure at all times their business continuity and to be able to provide high quality services to their			

PUBLIC

clients, the dedicated interface that they are expected to use must meet high level requirements in terms of performance and functionalities. It should at a minimum ensure 'data parity' with the customer interface provided to its users by the account servicing payment service provider, therefore including the payment account data which is also available to the payment service users in the interface provided to them by the account servicing payment service provider. With regard to payment initiation services, the dedicated interface should allow not only the initiation of single payments but of standing orders and direct debits. More detailed requirements for dedicated interfaces should be laid down in Regulatory Technical Standards developed by the EBA.			
(60) Given the dramatic impact that a prolonged unavailability of a dedicated interface would have on account information and payment initiation service providers' business continuity, account servicing payment service providers should remedy such unavailability without delay. Account servicing payment service providers should	(60) Given the dramatic impact that a prolonged <u>unplanned</u> unavailability of a dedicated interface would have on account information and payment initiation service providers' business continuity, account servicing payment service providers should		

PUBLIC

inform account information and payment initiation service providers of any such unavailability of their dedicated interface and of the measures taken to remedy them without delay. In case of unavailability of a dedicated interface, and where no effective alternative solution is offered by the account servicing payment service provider, account information and payment initiation service providers should be able to preserve their business continuity. They should be allowed to request their national competent authority to make use of the interface provided to its users by the account servicing payment service provider until the dedicated interface is again available. The competent authority should, upon receiving the request, take its decision without delay. Pending the decision from the authority the requesting account information and payment initiation service providers should be allowed to temporarily use the interface provided to its users by the account servicing payment service provider. The relevant competent authority should set a deadline to the account servicing payment service provider to restore the full functioning of the dedicated interface, with	remedy such unavailability without delay and should ensure an optimal recovery time of the dedicated interface. Account servicing payment service providers should inform account information and payment initiation service providers of any such unavailability of their dedicated interface and of the measures taken to remedy them without delay. Given the paramount importance of full availability and functionality of the dedicated interface for the business models of account information and payment initiation service providers, the dedicated interface should ensure availability and performance that equals at least that of the interface that the account servicing payment service provider uses for authentication and communication with its users The EBA is mandated to clarify the requirements related to the quarterly statistics on the availability and performance of dedicated interfaces		

PUBLIC

the possibility of sanctions in case of failure to do so by the deadline. All account information and payment initiation service providers, not just those which introduced the request, should be allowed to access the data they need to ensure their business continuity.	(and, for comparison purposes, of the interfaces that the account servicing payment service provider makes available to its payment service users for directly accessing their payment account online) and the publication thereof on the website of the account servicing payment service provider and the standards establishing an optimal recovery time in case of dedicated interface unplanned unavailability, based on the severity of the incident. Said severity should take into account, among others, the number of customers impacted and types of functionality affected of account information and payment initiation service providers. ~~In case of unavailability of a dedicated interface, and where no effective alternative solution is offered by the account servicing payment service provider, account information and payment initiation service providers should be able to preserve their business continuity.~~		

PUBLIC

	~~They should be allowed to request their national competent authority to make use of the interface provided to its users by the account servicing payment service provider until the dedicated interface is again available. The competent authority should, upon receiving the request, take its decision without delay. Pending the decision from the authority the requesting account information and payment initiation service providers should be allowed to temporarily use the interface provided to its users by the account servicing payment service provider. The relevant competent authority should set a deadline to the account servicing payment service provider to restore the full functioning of the dedicated interface, with the possibility of sanctions in case of failure to do so by the deadline. All account information and payment initiation service providers, not just those which introduced the request, should be~~		

PUBLIC

	~~allowed to access the data they need to ensure their business continuity.~~		
(61) Such temporary direct access should have no negative effect on consumers. Account information and payment initiation service providers should therefore always duly identify themselves and respect all their obligations, such as the limits of the permission which was granted to them, and should in particular access only the data that they need to meet their contractual obligations and provide the regulated service. Access to payments account data without proper identification (so-called 'screen-scraping') should, in any circumstances, never be performed.	(61) ~~Such temporary direct access should have no negative effect on consumers.~~ Account information and payment initiation service providers should ~~therefore~~ always duly identify themselves and respect all their obligations, such as the limits of the permission which was granted to them, and should in particular access only the data that they need to meet their contractual obligations and provide the regulated service. Access to payments account data without proper identification (so-called 'screen-scraping') should, in any circumstances, never be performed.		
(62) Given the fact that setting up a dedicated interface could, for certain account servicing payment service providers, be deemed disproportionately burdensome, a national competent authority should be able to exempt an account servicing payment service provider, on its request, from the obligation to have in place a dedicated data	(62) Given the fact that setting up or maintaining a dedicated interface could, for certain account servicing payment service providers, be deemed disproportionately burdensome, a national competent authority should be able to exempt an account servicing payment service	(62) Given the fact that setting up or maintaining a dedicated interface could, for certain account servicing payment service providers, be deemed disproportionately burdensome, a Member State	

PUBLIC

access interface, and to either offer payment data access only via its 'customer interface' or not to offer any open banking data access interface at all. Data access via the customer interface (with no dedicated interface) may be appropriate in the case of a very small account servicing payment service provider for which a dedicated interface would be a significant financial and resource burden. Being exempted from the obligation to maintain any 'open banking' data access interface may be justified where the account servicing payment service provider has a specific business model, for example where open banking services would present no relevance to its customers. Detailed criteria for granting such different types of exemption decisions should be laid down in regulatory technical standards developed by the EBA.	provider, on its request, from the obligation to have in place a dedicated data access interface, and to either offer payment data access only via its 'customer interface' provided this interface is already an API endpoint or not to offer any open banking data access interface at all. Data access via the customer interface (with no dedicated interface) may be appropriate where this interface is already an API, such as in B2B business cases where no mobile applications or website interfaces are used between the account servicing payment service provider and its customer, and where ~~in the case of a very small account servicing payment service provider for which~~ a dedicated interface would be a significant financial and resource burden for the account servicing payment service provider. Being exempted from the obligation to maintain any 'open banking' data access interface may be justified where the account servicing payment	or a national competent authority should be able to exempt an account servicing payment service provider, on its request, from the obligation to have in place a dedicated data access interface, and to either offer payment data access only via its 'customer interface' provided this interface is already an API endpoint or not to offer any open banking data access interface at all. Data access via the customer interface (with no dedicated interface) may be appropriate where this interface is already an API, such as in B2B business cases where no mobile applications or website interfaces are used between the account servicing payment service provider and its customer, and where ~~in the case of a very small account servicing~~	

	service provider has a specific business model, for example where open banking services would present no relevance to its customers. Detailed criteria for granting such different types ofexemption decisions should be laid down in regulatory technical standards developed by the EBA, taking into account inter alia the size, annual turnover and payments volume of the account servicing payment service provider. It should be noted that such an exemption, once granted, cannot be perpetuated if the circumstances which led to the exemption changed significantly.	~~payment service provider for which~~ a dedicated interface would be a significant financial and resource burden for the account servicing payment service provider. Being exempted from the obligation to maintain any 'open banking' data access interface may be justified where the account servicing payment service provider has a specific business model, for example where open banking services would present no relevance to its customers. Detailed criteria for granting such different types ofexemption decisions should be laid down in regulatory technical standards developed by the EBA, taking into account inter alia the size, annual turnover and payments volume of the account servicing payment service	

		provider. It should be noted that such an exemption, once granted, cannot be perpetuated if the circumstances which led to the exemption changed significantly. ***[PRES comment:*** *Amendments based on the non-paper of one of the Member States reflecting specific national cirucmstances.]*	
(63) To fully reap the potential of open banking in the Union, it is essential to prevent any discriminatory treatment of account information and payment initiation service providers by account servicing payment service providers. Where the payment service user has decided to make use of the services of an account information service provider or a payment initiation service provider, the account servicing payment service provider should treat that order in the same way as it would treat such a request if made by the payment service user directly in			

PUBLIC

its 'customer interface', unless the account servicing payment provider has objective reasons to treat the request to access the account differently, including serious suspicions of fraud.			
(64) For the provision of payment initiation services, the account servicing payment service provider should provide the payment initiation service provider with all information accessible to it regarding the execution of the payment transaction immediately after the payment order has been received. Sometimes more information becomes available to the account servicing payment service provider after it has received the payment order, but before it has executed the payment transaction. Where relevant for the payment order and the execution of the payment transaction, the account servicing payment service provider should provide that information to the payment initiation service provider. The payment initiation service provider should benefit from the information necessary to assess the risks of non-execution of the initiated transaction. That information is indispensable to enable the payment			

PUBLIC

initiation service provider to offer to a payee on behalf of whom it initiates the transaction a service whose quality can compete with other means of electronic payments available to the payee, including payment cards.			
(65) To increase trust in open banking, it is essential that payment service users who use account information and payment initiation services be in full control of their data and have access to clear information on the data access permissions that those payment service users have granted to payment service providers, including the purpose of permission and the categories of payment account data concerned, including identity data of the account, transaction and account balance. Account servicing payment service providers should therefore make available to payment service users who use such services a 'dashboard', for monitoring and withdrawing or re-establishing data access granted to 'open banking' services providers. Permissions for initiation of one-off payments should not feature on that dashboard. A dashboard may not allow a payment service user to establish new data	(65) To increase trust in open banking, it is essential that payment service users who use account information and payment initiation services be in full control of their data and have access to clear information on the data access permissions that those payment service users have granted to payment service providers, including the purpose of permission and the categories of payment account data concerned, including identity data of the account, transaction and account balance. Account servicing payment service providers should therefore make available to payment service users who use such services a 'dashboard', for monitoring and withdrawing or re-establishing <u>(for example, in case of errors made)</u> data access granted to		

PUBLIC

access permissions with an account information or payment initiation service provider to which no previous data access has been given. Account servicing payment service providers should inform account information and payment initiation service providers promptly of any withdrawal of data access. Account information and payment initiation service providers should inform account servicing payment service providers promptly of new and re-established data access permissions granted by payment service users, including the duration of validity of the permission and its purpose (in particular whether the consolidation of data is for the benefit of the user or for transmission to a third party). An account servicing payment service provider should not encourage, in any manner, a payment service user to withdraw the permissions given to account information and payment initiation service providers. The dashboard should warn the payment service user in a standard way of the risk of possible contractual consequences of withdrawal of data access to an open banking service provider, since the dashboard does not	'open banking' services providers. The dashboards should not contain any deterring or discouraging language that might dissuade the payment service user from making use of the services of a payment initiation service provider or account information service provider. Permissions for initiation of one-off payments should not feature on that dashboard. A dashboard may not allow a payment service user to establish new data access permissions with an account information or payment initiation service provider to which no previous data access has been given. Account servicing payment service providers should inform account information and payment initiation service providers promptly of any withdrawal of data access and within 24 hours at the latest. Account information and payment initiation service providers should inform account servicing payment service providers promptly of new and re-established data access		

PUBLIC

manage the contractual relationship between the user and an 'open banking' provider, but it is for the payment service user to verify that risk. A permissions dashboard should empower customers to manage their permissions in an informed and impartial manner and give customers a strong measure of control over how their personal and non-personal data is used. A permissions dashboard should take into account, where appropriate, the accessibility requirements under Directive (EU) 2019/882 of the European Parliament and of the Council.	permissions granted by payment service users, including the duration of validity of the permission and its purpose (in particular whether the consolidation of data is for the benefit of the user or for transmission to a third party). An account servicing payment service provider should not encourage, in any manner, a payment service user to withdraw the permissions given to account information and payment initiation service providers. The dashboard should warn the payment service user in a standard way of the risk of possible contractual consequences of withdrawal of data access to an open banking service provider, since the dashboard does not manage the contractual relationship between the user and an 'open banking' provider, but it is for the payment service user to verify that risk. A permissions dashboard should empower customers to manage their permissions in an informed and impartial manner and give customers		

PUBLIC

	a strong measure of control over how their personal and non-personal data is used. A permissions dashboard should take into account, where appropriate, the accessibility requirements under Directive (EU) 2019/882 of the European Parliament and of the Council.		
	(65a) Account information service providers should be able to access information on designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of providing the account information service, where the payment service user does not actively request such information, but the payment service user has given his consent. In this case, the payment service user must be informed by the account information service provider, but this information obligation does not have to be fulfilled on an access by access basis, but may be fulfilled by including this information in the		

PUBLIC

	framework contract between the account information service provider and the payment service user.		
(66) The review of Directive (EU) 2015/2366 has revealed that account information and payment initiation service providers are still exposed to many unjustified obstacles, despite the level of harmonisation achieved and of the prohibition on such obstacles imposed by Article 32(3) of Commission Delegated Regulation (EU) 2018/389[19]. Those obstacles still significantly hamper the full potential of open banking in the Union. Those obstacles are regularly reported by account information and payment initiation service providers to supervisors, regulators and the Commission. They were analysed by the EBA in its June 2020 Opinion on "*Obstacles to the provision of third-party provider services under the Payment Services Directive*". Despite clarifications efforts made there is still a lot of uncertainty, in the market and with supervisors, as to what			

[19] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (OJ L 69, 13.3.2018, p. 23).

PUBLIC

constitutes a 'prohibited obstacle' to regulated open banking services. It is therefore indispensable to provide a clear and non-exhaustive list of such prohibited open banking obstacles, relying in particular on the work carried out by the EBA.			
(67) The obligation to keep personalised security credentials safe is of the utmost importance to protect the funds of the payment service user and to limit the risks relating to fraud and unauthorised access to payment accounts. However, terms and conditions or other obligations imposed by payment service providers on payment service users in relation to keeping personalised security credentials safe should not be drafted in a way that prevents payment service users from taking advantage of services offered by other payment service providers, including payment initiation services and account information services. Such terms and conditions should not contain any provisions that would make it more difficult, in any way, to use the payment services of other payment service providers authorised or registered pursuant to Directive			

PUBLIC

(EU) XXX (PSD3). Furthermore, it is appropriate to specify that, for the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.			
(68) To be fully successful, 'open banking' requires a robust and effective enforcement of the rules that regulate that activity. As there exists no single authority at the level of the Union to enforce 'open banking' rights and duties, national competent authorities are the first level of open banking enforcement. It is essential that national competent authorities proactively and rigorously ensure the respect of the Union 'open banking' regulated framework. Insufficient enforcement by the relevant authorities is regularly presented by open banking operators as being one of the reasons for its still limited take-up in the Union. National competent authorities should have the appropriate resources to perform their enforcement tasks effectively and efficiently. National competent authorities should	(68) To be fully successful, 'open banking' requires a robust and effective enforcement of the rules that regulate that activity. As there exists no single authority at the level of the Union to enforce 'open banking' rights and duties, national competent authorities are the first level of open banking enforcement. It is essential that national competent authorities ~~proactively and rigorously~~ ensure the respect of the Union 'open banking' regulated framework. ~~Insufficient enforcement by the relevant authorities is regularly presented by open banking operators as being one of the reasons for its still limited take-up in the Union. National competent authorities~~		

PUBLIC

promote and broker a smooth and regular dialogue between the various actors of the 'open banking' ecosystem. Account servicing payment service providers and account information and payment initiation service providers which do not comply with their obligations should be subjected to appropriate sanctions. Regular monitoring of the 'open banking' market in the Union by competent authorities, coordinated by the EBA, should facilitate enforcement, and collection of data on the 'open banking' market will remedy a data gap which currently exists, hampering any effective measurement of the actual take-up of 'open banking' in the Union. Account servicing payment service providers and account information and payment initiation service providers should have access to dispute settlement bodies, pursuant to Article 10 of the Data Act proposal, once that Regulation enters into force.	~~should have the appropriate resources to perform their enforcement tasks effectively and efficiently~~. National competent authorities ~~should~~ are in a good position to promote and broker a smooth and regular dialogue between the various actors of the 'open banking' ecosystem. Account servicing payment service providers and account information and payment initiation service providers which do not comply with their obligations should be subjected to appropriate sanctions. Regular monitoring of the 'open banking' market in the Union by competent authorities, coordinated by the EBA, should facilitate enforcement, and collection of data on the 'open banking' market will remedy a data gap which currently exists, hampering any effective measurement of the actual take-up of 'open banking' in the Union. Account servicing payment service providers and account information and payment initiation service providers should have access		

PUBLIC

	to dispute settlement bodies, pursuant to Article 10 of Regulation (EU) 2023/2854 of the European Parliament and of the Council (the Data Act) ~~proposal, once that Regulation enters into force~~.		
(69) The parallel use of the term 'explicit consent' in Directive (EU) 2015/2366 and Regulation (EU) 2016/679 of the European Parliament and of the Council[20] has led to misinterpretations. The object of the explicit consent under Article 94 (2) of Directive (EU) 2015/2366 is the permission to obtain access to those personal data, to be able to process and store these personal data that are necessary for the purpose of providing the payment service. Therefore, a clarification should be made to increase legal certainty and have a clear differentiation with data protection rules. Where the term 'explicit consent' was used in Directive (EU) 2015/2366, the term 'permission' should be used in the present Regulation. When reference is made to 'permission' that	(69) ~~The parallel use of the term 'explicit consent' in Directive (EU) 2015/2366 and Regulation (EU) 2016/679 of the European Parliament and of the Council has led to misinterpretations. The object of the explicit consent under Article 94 (2) of Directive (EU) 2015/2366 is the permission to obtain access to those personal data, to be able to process and store these personal data that are necessary for the purpose of providing the payment service. Therefore, a clarification should be made to increase legal certainty and have a clear differentiation with data protection rules. Where the term 'explicit consent' was used in~~	(69) ~~The parallel use of the term 'explicit consent' in Directive (EU) 2015/2366 and Regulation (EU) 2016/679 of the European Parliament and of the Council has led to misinterpretations. The object of the explicit consent under Article 94 (2) of Directive (EU) 2015/2366 is the permission to obtain access to those personal data, to be able to process and store these personal data that are necessary for the purpose of providing the payment service. Therefore, a~~	

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

reference should be without prejudice to obligations of payment service providers under Article 6 of Regulation (EU) 2016/679. Therefore, permission should not be construed exclusively as 'consent' or 'explicit consent' as defined in Regulation (EU) 2016/679.	~~Directive (EU) 2015/2366, the term 'permission' should be used in the present Regulation. When reference is made to 'permission' that reference should be without prejudice to obligations of payment service providers under Article 6 of Regulation (EU) 2016/679. Therefore, permission should not be construed exclusively as 'consent' or 'explicit consent' as defined in Regulation (EU) 2016/679.~~ The notion of consent under this Regulation is without prejudice to the rules on lawful processing of personal data, including provisions on 'consent' and 'explicit consent', laid out in Regulation (EU) 2016/679 of the European Parliament and of the Council. Where processing of personal data is involved, it is the responsibility of the data controller to assess the appropriate legal basis under Regulation (EU) 2016/679 and ensure that all conditions for this legal basis laid out in that Regulation are met.	~~clarification should be made to increase legal certainty and have a clear differentiation with data protection rules. Where the term 'explicit consent' was used in Directive (EU) 2015/2366, the term 'permission' should be used in the present Regulation. When reference is made to 'permission' that reference should be without prejudice to obligations of payment service providers under Article 6 of Regulation (EU) 2016/679. Therefore, permission should not be construed exclusively as 'consent' or 'explicit consent' as defined in Regulation (EU) 2016/679.~~ The notion of consent under this Regulation is without prejudice to the rules on lawful processing of personal data, including provisions on	

	Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the use of a payment instrument in the form agreed by the payment service provider and the payment service user, is in itself not be sufficient to prove either that the payment transaction was authorised by the payer. This means that the authentication or the use of the strong customer authentication recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52.	'consent' and 'explicit consent', laid out in Regulation (EU) 2016/679 of the European Parliament and of the Council. Where processing of personal data is involved, it is the responsibility of the data controller to assess the appropriate legal basis under Regulation (EU) 2016/679 and ensure that all conditions for this legal basis laid out in that Regulation are met. Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the use of a payment instrument in the form agreed by the payment service provider and the payment service user, is in itself not ~~be~~ sufficient to prove either that the payment transaction was authorised by	

		the payer. This means that the authentication or the use of the strong customer authentication recorded by the payment service provider, including the payment initiation service provider as appropriate, ~~shall~~ should in itself not be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52.	
	(69xx) Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the use of a payment instrument in the form agreed by the payment service provider and the payment service user, is in itself not sufficient to prove		

PUBLIC

	either that the payment transaction was authorised by the payer. This means that the authentication or the use of the strong customer authentication recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52.		
	(69a) Authorisation is based on an intention or a contribution in fact. If the payment service user uses its security credentials in a responsible manner when executing a payment transaction, the validity and authenticity of the authorisation will be easier to assess. The set of payment transactions can be divided into two distinct categories, those that are considered authorised and those		

PUBLIC

	that are not, called unauthorised. The payment transaction operates as a process and requires the active participation and approval of the payment service user.		
	(69b) The payment service provider's decisions shall be based on "objectively justified reasons" based on the data acquired through the transaction monitoring mechanism, and shall take into account the risks of frauds that could jeopardize the safety of the payment instrument and the interest of the payment service user. Examples for "objectively justified reasons" might include suspicion of unauthorized use, suspicion of fraudulent transactions, security of payment instrument, risk of deception regarding financial activity and large distance transactions in unjustifiably short timeframe.		
	(69c) Where based on transaction monitoring the payer's PSP suspects that the payer may be a victim of	(69a) Where based on transaction monitoring the payer's payment service	

	fraud, before suspending the execution of the payment transaction pursuant to Article 71 AMLR, the payer's PSP should without undue delay make reasonable efforts to communicate with the payer in a manner agreed in the framework contract to assess whether the fraud suspicion is justified or not. Without prejudice to the obligation under Article 73 AMLR not to disclose that information is being or will be transmitted to the Financial Intelligence Unit.	provider suspects that the payer may be a victim of fraud, before suspending the execution of the payment transaction pursuant to Article 71 AMLR, the payer's payment service provider should without undue delay make reasonable efforts to communicate with the payer in a manner agreed in the framework contract to assess whether the fraud suspicion is justified or not. Without prejudice to the obligation under Article 73 AMLR not to disclose that information is being or will be transmitted to the Financial Intelligence Unit.	
		(69d) It is important to ensure that payment service providers' transaction monitoring mechanisms are effective in preventing fraud, while mitigating the impact	

		on legitimate payment transactions and customer detriment deriving from delays in the execution of legitimate payment transactions or the blocking of such transactions. For the purpose of this Regulation, the fact that a payment order is unusual should not automatically constitute grounds for suspecting that the payment transaction is fraudulent, nor should it by itself constitute reasonable grounds to suspect fraud. In assessing whether there are reasonable grounds to suspect fraud in relation to a payment transaction, the payment service provider should take into account the specific circumstances of the individual transaction, together with the payment service provider's wider assessment of evolving fraud	

		risk based on the payment service provider's transaction monitoring and on any other relevant information available to the payment service provider. Where the payment service provider has duly justified and reasonable grounds to suspect fraud, a refusal in good faith to execute or postpone a payment transaction should not involve the payment service provider in liability of any kind.	
(70) Security of credit transfers is fundamental for increasing the confidence of payment service users in such services and ensuring their use. Payers intending to send a credit transfer to a given payee may, as a result of fraud or error, provide a unique identifier which does not correspond to an account held by that payee. To contribute to the reduction of fraud and errors, payment service users should benefit from a service			

PUBLIC

which would verify whether there is any discrepancy between the unique identifier of the payee and the name of the payee provided by the payer and, should any such discrepancies be detected, notify the payer thereof. Such services, in the countries where they exist, have had a substantial positive impact on the level of fraud and errors. Given the importance of that service for the prevention of fraud and errors, such service should be available free of charge to consumers. To avoid undue frictions or delays in the processing of the transaction, the payment service provider of the payer should provide such notification within no more than a few seconds from the moment the payer has entered the payee information. To enable the payer to decide whether to proceed with the intended transaction, the payment service provider of the payer should provide such notification before the payer authorises the transaction. Certain credit transfer initiation solutions may be available to payers allowing them to place a payment order without inserting themselves the unique identifier. Instead, such data elements are provided by the provider of that initiation			

PUBLIC

solution. In such cases, there is no need for a service verifying the match between the unique identifier and the name of the payee since the risk of fraud or errors is significantly reduced.			
(71) Regulation (EU) XXX amending Regulation (EU) No 260/2012 provides for a service verifying the match between the unique identifier and the name of the payee to be offered to users of instant credit transfers in euro. To achieve a coherent framework for all credit transfers whilst avoiding any undue overlap, the verification service referred to in the present Regulation should only apply to credit transfers which are not covered by Regulation (EU) XXX amending Regulation (EU) No 260/2012.			
(72) Some attributes of the name of the payee to whose account the payer wishes to make a credit transfer may increase the likelihood of a discrepancy being detected by the payment service provider, including the presence of diacritics or different possible transliterations of names in different alphabets, differences between habitually used names and names indicated on formal			

PUBLIC

identification documents in case of natural persons, or differences between commercial and legal names in case of legal persons. To avoid undue frictions in the processing of credit transfers and facilitate the payer's decision on whether to proceed with the intended transaction, payment service providers should indicate the degree of such discrepancy by indicating in the notification where there is no match or a 'close' match.			
(73) Authorising a payment transaction despite the matching verification service having detected a discrepancy and notified that discrepancy to the payment service user can result in the funds being transferred to an unintended payee. Payment service providers should inform payment service users about the possible consequences of their choice to ignore the notified discrepancy and proceed with the execution of the transaction. Payment service users should be able to opt out from using such a service at any time during their contractual relationship with the payment service provider. After opting out, payment service users should be able to avail again of the service.			

PUBLIC

	(73a) In the Regulation there is a new requirement for both the PSP and the PSU to embrace a good-faith cooperation with the aim of mitigating the impact of the escalating fraudulent payment transactions, moreover to ensure that the PSU has additional means to protect itself at the level of the tools used. The PSU is expected to adopt a preventive conduct and to exercise alertness in its relation to the PSP. In spite of the PSP and the PSU having distinct roles in the prevention there are security measures to be taken jointly. The PSU is dependent on the supplementary services provided by the PSP. In the event of a fraudulent payment transaction, the PSP is obliged to investigate the fraud event in accordance with the data obtained from its own information technology resources and the information provided by the PSU.		
(74) The payment service user should inform the payment service provider as soon			

PUBLIC

as possible about any contestations concerning allegedly unauthorised, incorrectly executed payment transactions or authorised credit transfers where there was a malfunctioning of the matching verification service, provided that the payment service provider has fulfilled its information obligations. If the notification deadline has been met by the payment service user, the payment service user should be able to pursue those claims subject to national limitation periods. That should not affect other claims between payment service users and payment service providers.			
(75) Provision should be made for the allocation of losses in the case of unauthorised payment transactions or of specific authorised credit transfers. Different provisions may apply to payment service users who are not consumers, since such users are normally in a better position to assess the risk of fraud and take countervailing measures. To ensure a high level of consumer protection, payers should always be entitled to address their claim to a refund to their account servicing payment			

PUBLIC

service provider, even where a payment initiation service provider is involved in the payment transaction. That should be without prejudice to the allocation of liability between the payment service providers.			
(76) In the case of payment initiation services, the allocation of liability between the payment service provider servicing the account and the payment initiation service provider involved in the transaction should compel them to take responsibility for the respective parts of the transaction that are under their control.			
(77) In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payer and where that suspicion is based on objective grounds which are communicated to the relevant national authority by the payment service provider, the payment service provider should be able to conduct an investigation before refunding the payer. The payment	(77) In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payer and where that suspicion is based on objective grounds which are communicated to the relevant national authority by the payment service provider, the payment service provider should be		

PUBLIC

service provider should, within 10 business days after noting or being notified of the transaction, either refund the payer the amount of the unauthorised payment transaction or provide the payer the reasons and supporting evidence for refusing the refund and indicate the bodies to which the payer may refer the matter if the payer does not accept the reasons provided. To protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount was debited. To provide an incentive for the payment service user to notify, without undue delay, the payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount unless the payment service user has acted fraudulently or with gross negligence. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not able to become aware of the loss, theft or misappropriation of the payment instrument.	able to conduct an investigation before refunding the payer. The payment service provider should, within ~~10~~ 15 business days after noting or being notified of the transaction, either refund the payer the amount of the unauthorised payment transaction or provide the payer the reasons and supporting evidence for refusing the refund and indicate the bodies to which the payer may refer the matter if the payer does not accept the reasons provided. To protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount was debited. To provide an incentive for the payment service user to notify, without undue delay, the payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount unless the payment service user has acted fraudulently or with		

PUBLIC

Moreover, once a payment service user has notified a payment service provider that his or her payment instrument may have been compromised, the payment service user should not be required to cover any further losses stemming from unauthorised use of that instrument. Payment service providers should be responsible for the technical security of their own products.	gross negligence. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not able to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once a payment service user has notified a payment service provider that his or her payment instrument may have been compromised, the payment service user should not be required to cover any further losses stemming from unauthorised use of that instrument. Payment service providers should be responsible for the technical security of their own products.		
(78) Liability provisions in the case of authorised credit transfers where there was an incorrect application or malfunctioning of the service detecting discrepancies between the name and unique identifier of a payee would create the right incentives for payment			

PUBLIC

service providers to provide a fully functioning service, with the aim of reducing the risk of ill-informed payment authorisations. If the payer decided to make use of such a service, the payment service provider of the payer should be held liable for the full amount of the credit transfer in cases where that payment service provider failed, whereas it should have done so if properly functioning, to notify the payer of a discrepancy between the unique identifier and the name of the payee provided by the payer and such failure caused a financial damage to the payer. Where the liability of the payment service provider of the payer is attributable to the payment service provider of the payee, the payment service provider of the payee should compensate the payment service provider of the payer for the financial damage incurred.			
(79) Consumers should be adequately protected in the context of certain fraudulent payment transactions that they have authorised without knowing these transactions were fraudulent. The number of 'social engineering' cases where consumers	(79) Consumers should be adequately protected in the context of certain fraudulent payment transactions that they have ~~authorised~~ <u>authenticated</u> without knowing these transactions were fraudulent. The number of	(79) Consumers should be adequately protected in the context of certain fraudulent payment transactions that they have authorised without knowing these transactions	

are misled into authorising a payment transaction to a fraudster has significantly increased in recent years. 'Spoofing' cases where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name, mail address or telephone number to gain the customers' trust and trick them into carrying-out some actions, are unfortunately becoming more widespread in the Union. Those new types of 'spoofing' fraud are blurring the difference that existed in Directive (EU) 2015/2366 between authorised and unauthorised transactions. Means through which the consent may be assumed to be granted are also becoming more complex to identify, as fraudsters can take control of the whole consent and authentication process including of the strong customer authentication completion. The conditions under which the customer authorised a transaction by giving his or her permission to it should be taken into due consideration, including by courts, to qualify a transaction as being authorised or unauthorised. A transaction may indeed have been authorised in circumstances where such	'social engineering' cases where consumers are misled into ~~authorising~~ authentication of a payment transaction to a fraudster has significantly increased in recent years. ~~'Spoofing' cases where fraudsters pretend to be employees of a customer's payment service provider~~ Social engineering cases are for example 'spoofing' cases where fraudsters pretend to be another person or entity, such as the consumer's payment service provider, a tax authority, or a trusted person known by the consumer and misuse the payment service provider's name, mail address or telephone number to gain the customers' trust and trick them into carrying-out some actions, are unfortunately becoming more widespread in the Union. Those new types of ~~'spoofing'~~ fraud are blurring the difference that existed in Directive (EU) 2015/2366 between authorised and unauthorised transactions. Means through which	were fraudulent. The number of 'social engineering' cases where consumers are manipulated ~~misled~~ into authorising a payment transaction to a fraudster has significantly increased in recent years. 'Spoofing' cases where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name, mail address or telephone number to gain the customers' trust and trick them into carrying-out some actions, are unfortunately becoming more widespread in the Union. Those new types of 'spoofing' fraud are blurring the difference that existed in Directive (EU) 2015/2366 between authorised and unauthorised transactions. Means through which the consent may be	

authorisation was granted on manipulated premises affecting the integrity of the permission. It is therefore no longer possible, as was the case in Directive (EU) 2015/2366, to limit refunds to unauthorised transactions only. It would however be disproportionate and financially very costly to payment services providers to open every fraudulent transaction, authorised or unauthorised, to a systematic refund right. It might also cause moral hazard and a reduction in the customer's vigilance.	the consent may be assumed to be granted are also becoming more complex to identify, as fraudsters can take control of the whole consent and authentication process including of the strong customer authentication completion. The conditions under which the customer ~~authorised~~ authenticated a transaction by giving his or her ~~permission~~ consent to it should be taken into due consideration, including by courts, to qualify ~~a transaction as being authorised or unauthorised~~ a consent of the customer as a valid, non manipulated consent. A transaction may indeed have been ~~authorised~~ authenticated in circumstances where such ~~authorisation~~ authentication was granted on manipulated premises affecting the integrity of the ~~permission~~ consent. It is therefore no longer possible, as was the case in Directive (EU) 2015/2366, to limit refunds to unauthorised transactions only. It would however be disproportionate and financially very	assumed to be granted are also becoming more complex to identify, as fraudsters can take control of the whole consent and authentication process including of the strong customer authentication completion. The conditions under which the customer authorised a transaction by giving his or her ~~permission~~ consent to it should be taken into due consideration, including by courts, to qualify a transaction as being authorised or unauthorised. A transaction may indeed have been authorised in circumstances where such authorisation was granted on manipulated premises affecting the integrity of the ~~permission~~ consent. It is therefore no longer possible, as was the case in Directive (EU) 2015/2366, to limit	

	costly to payment services providers to open every fraudulent transaction, ~~authorised or unauthorised~~, to a systematic refund right. It might also cause moral hazard and a reduction in the customer's vigilance.	refunds to unauthorised transactions only. It would however be disproportionate and financially very costly to payment services providers to open every fraudulent transaction, authorised or unauthorised, to a systematic refund right. It might also cause moral hazard and a reduction in the customer's vigilance. *[**PRES comment:** Proposal presented at the February CWP meeting.]*	
(80) Payment service providers could be also considered as victims of 'spoofing' cases, as their details were usurped. However, payment service providers have more means than consumers to put an end to these fraud cases, through adequate prevention and robust technical safeguards developed with electronic communications services providers such as mobile network operators, internet platforms etc. Cases of bank employee impersonation fraud affect	(80) Payment service providers could be also considered as victims of 'spoofing' cases, as their details were usurped. However, payment service providers have more means than consumers to put an end to these fraud cases, through adequate prevention and robust technical safeguards developed with electronic communications services providers such as mobile network operators,		

PUBLIC

the good repute of the bank, of the banking sector as a whole and may cause significant financial damages to Union consumers, affecting their trust in electronic payments and in the banking system. A good-faith consumer who has been the victim of such 'spoofing' fraud where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name, mail address or telephone number should therefore be entitled to a refund of the full amount of the fraudulent payment transaction from the payment service provider, unless the payer has acted fraudulently or with 'gross negligence'. As soon as the consumer becomes aware that he or she has been a victim of that type of spoofing fraud, the consumer should without undue delay report the incident to the police, preferably via online complaint procedures, where made available by the police, and to his or her payment service provider, providing every necessary supporting evidence. No refund should be granted where those procedural conditions are not fulfilled.	internet platforms etc. Fraudsters often rely on tools and techniques such as caller ID, e-mail address, or IP address spoofing. Such fraud cases are therefore complex, oftentimes involving different actors along the fraud scheme chain. Payment service providers and electronic communications services providers can both play a critical role in the prevention of payment fraud. Providers of electronic communications services such as mobile network operators have specific obligations with regard to the availability, authenticity, integrity, or confidentiality of communications under Directive 2002/58/EC and Directive (EU) 2018/1972. It is essential that payment service providers and electronic communications services providers cooperate closely and combine their respective technical means to prevent payment fraud, taking into account their respective responsibilities and		

PUBLIC

	obligations, notably under the aforementioned regulations.		
	(80a) Cases of bank employee impersonation (spoofing) fraud affect the good repute of the bank financial entity, of the banking financial sector as a whole and may cause significant financial damages to Union consumers, affecting their trust in electronic payments and in the banking financial system. A good-faith consumer who has been the victim of such manipulated transactions, namely 'spoofing' fraud where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name, mail address or telephone number should therefore be entitled to a refund of the full amount of the fraudulent payment transaction from the payment service provider on a shared-damage basis, unless the payer has acted fraudulently or with 'gross negligence'. As soon as the		

PUBLIC

	consumer becomes aware that he or she has been a victim of that type of spoofing fraud manipulation, the consumer should without undue delay report the incident to the police, preferably via online complaint procedures, where made available by the police, and to his or her payment service provider, providing every necessary supporting evidence. No refund should be granted where those procedural conditions are not fulfilled. Although the payment service provider may have perceived the payment transaction as authorised, the customer was the victim of a fraud, so in order to establish customer protection and maintain trust in the financial system, a properly designed damage sharing can ensure a real balance between the interests of the consumer and the payment service provider in such manipulation cases. Without prejudice to the right of customers to bring action in courts, the rules of refunds based on shared		

PUBLIC

	compensation between the payer and the payment service provider can only be considered as a temporary (preliminary) way.		
(81) Given their obligations to safeguard the security of their services in accordance with Directive 2002/58/EC of the European Parliament and of the Council[21], electronic communications services providers have the capacity to contribute to the collective fight against 'spoofing' fraud. Therefore, and without prejudice to the obligations laid down in national law implementing that Directive, electronic communications services providers should cooperate with payment service providers with a view to preventing further occurrences of that type of fraud, including by acting promptly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC. Any claim by a payment service provider against other			

[21] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31.7.2002, p.37).

PUBLIC

providers, such as electronic communications services providers, for financial damage caused in the context of this type of fraud should be made in accordance with national law.			
(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. The fact that a consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again	(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties, revealing or giving away any identification data or credentials which are necessary for	(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the	

victim of the same type of fraud could be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent *modus operandi*.	authentication of a payment transaction. The fact that a consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent *modus operandi*.	payment instrument in a format that is open and easily detectable by third parties, revealing or giving away any identification data or credentials which are necessary for authentication of a payment transaction. The fact that a consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent *modus operandi*.	

PUBLIC

(83) Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer, should be considered null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate to require the payment service provider to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases.			
(84) Consumers are particularly vulnerable in cases of card-based payment transactions where the exact transaction amount is not known at the moment when the payer gives permission to execute the payment transaction, for example at automatic fuelling stations, in car rental contracts or when making hotel reservations. The payer's payment service provider should be able to block an amount of funds on the payer's payment account in proportion with the amount of the payment transaction which			

PUBLIC

can reasonably be expected by the payer, and only if the payer has given his or her consent for that precise amount to be blocked. Those funds should be released immediately after receipt of the information on the exact final amount of the payment transaction and at the latest immediately after receipt of the payment order. To ensure a prompt release of the difference between the blocked amount and the exact amount of the payment transaction, the payee should inform the payment service provider immediately after the delivery of the service or goods to the payer.			
(85) Legacy non-euro direct debit schemes continue to exist in Member States whose currency is not the euro. Those schemes are proving to be efficient and ensure the same high level of protection to the payer by other safeguards, not always based on an unconditional right to a refund. In that case the payer should be protected by the general rule for a refund when the executed payment transaction exceeds the amount which could reasonably have been expected. In addition, it should be possible			

PUBLIC

for Member States to lay down rules concerning the right to a refund that are more favourable to the payer than those laid down in this Regulation. It would be proportionate to permit the payer and the payer's payment service provider to agree in a framework contract that the payer has no right to a refund in situations where the payer is protected. That might be either because the payer has given permission to execute a transaction directly to its payment service provider, including when the payment service provider acts on behalf of the payee, or because information on the future payment transaction was provided or made available in an agreed manner to the payer at least 4 weeks before the due date by the payment service provider or by the payee. In any event, the payer should be protected by the general refund rule in the case of unauthorised or incorrectly executed payment transactions or authorised credit transfers subject to an incorrect application of the matching verification service or in the case of payment service provider impersonation fraud.			

PUBLIC

(86) For financial planning and the fulfilment of payment obligations in due time, consumers and undertakings need to have certainty as to the length of time that the execution of a payment order will take. It is therefore necessary to establish when rights and obligations take effect, namely, when the payment service provider receives the payment order, including when the payment service provider has had the opportunity to receive it through the means of communication agreed in the payment service contract. This is notwithstanding any prior involvement in the process leading up to the creation and transmission of the payment order, including security and availability of funds checks, information on the use of the personal identity number or issuance of a payment promise. Furthermore, receipt of a payment order should occur when the payer's payment service provider receives the payment order to be debited from the payer's account. The time when a payee transmits to the payment service provider payment orders for the collection, for instance, of card payments or of direct debits or when the payee is granted a pre-			

PUBLIC

financing on the related amounts by the payment service provider by way of a contingent credit to the account should have no relevance in that respect. Users should be able to rely on the proper execution of a complete and valid payment order if the payment service provider has no contractual or statutory ground for refusal. If the payment service provider refuses a payment order, the refusal and the reason for the refusal should be communicated to the payment service user at the earliest opportunity, subject to the requirements of Union and national law. Where the framework contract provides that the payment service provider may charge a fee for refusal, such a fee should be objectively justified and should be as low as possible.			
(87) In view of the speed with which fully automated payment systems process payment transactions, which means that after a certain point in time payment orders cannot be revoked without high manual intervention costs, it is necessary to lay down a clear deadline for payment revocations. However, depending on the type of the payment service			

PUBLIC

and the payment order, it should be possible to vary the deadline for payment revocations by agreement between the parties. Revocation, in that context, should apply only between a payment service user and a payment service provider, and should be without prejudice to the irrevocability and finality of payment transactions in payment systems.			
(88) Irrevocability of a payment order should not affect a payment service provider's rights or obligations under the laws of Member States, based on the payer's framework contract or national laws, regulations, administrative provisions or guidelines, to reimburse the payer with the amount of the executed payment transaction in the event of a dispute between the payer and the payee. Such reimbursement should be considered to be a new payment order. Except for those cases, legal disputes arising within the relationship underlying the payment order should be settled only between the payer and the payee.			
(89) It is essential, for the fully integrated straight-through processing of payments and			

PUBLIC

for legal certainty with respect to the fulfilment of any underlying obligation between payment service users, that the full amount transferred by the payer should be credited to the account of the payee. Accordingly, it should not be possible for any of the intermediaries involved in the execution of payment transactions to make deductions from the amount transferred. However, it should be possible for payees to enter into an agreement with their payment service provider which allows the latter to deduct its own charges. Nevertheless, to enable the payee to verify that the amount due is correctly paid, subsequent information provided on the payment transaction should indicate not only the full amount of funds transferred, but also the amount of any charges that have been deducted.			
(90) To improve the efficiency of payments throughout the Union, all payment orders initiated by the payer and denominated in euro or the currency of a Member State whose currency is not the euro, including non-instant credit transfers and money remittances, should be subject to			

PUBLIC

a maximum 1-day execution time. For all other payments, such as payments initiated by or through a payee, including direct debits and card payments, in the absence of an explicit agreement between the payment service provider and the payer setting a longer execution time, the same 1-day execution time should apply. It should be possible to extend those periods by 1 additional business day, if a payment order is given on paper, to allow the continued provision of payment services to consumers who are used only to paper documents. When a direct debit scheme is used the payee's payment service provider should transmit the collection order within the time limits agreed between the payee and the payment service provider, enabling settlement on the agreed due date. It should be possible to maintain or establish rules specifying an execution time shorter than 1 business day.			
(91) The rules on execution for the full amount and execution time should constitute good practice where one of the payment service providers is not located in the Union. When making a credit transfer or money			

PUBLIC

remittance to a payee located outside the Union, the payment service provider of the payer should provide to the payer an estimation of the time needed for the credit transfer or money remittance to be credited to the payment service provider of the payee located outside the Union. A payment service provider in the Union cannot be expected to estimate the time taken by a payment service provider outside the Union to, after having received the funds, credit those funds to the account of the payee.			
(92) To strengthen their trust in payment markets, it is essential for payment service users to know the real charges of payment services. Accordingly, the use of non-transparent pricing methods should be prohibited, since it is commonly accepted that those methods make it extremely difficult for users to establish the real price of the payment service. Specifically, the use of value dating to the disadvantage of the user should not be permitted.			
(93) It should be possible for the payment service provider to specify unambiguously the information required to execute a			

PUBLIC

payment order correctly. The payment service provider of the payer should act with due diligence and verify, where technically possible and without requiring manual intervention, the coherence of the unique identifier, and, where the unique identifier is found to be incoherent, to refuse the payment order and inform the payer thereof.			
(94) The smooth and efficient functioning of payment systems depends on the user being able to rely on the payment service provider executing the payment transaction correctly and within the agreed time. Usually, the payment service provider is able to assess the risks involved in a payment transaction. It is the payment service provider that provides the payments system that makes arrangements to recall misplaced or wrongly allocated funds and decides in most cases on the intermediaries involved in the execution of a payment transaction. In view of all of those considerations, it is appropriate, except under abnormal and unforeseeable circumstances, to impose liability on the payment service provider in respect of the execution of a payment			

PUBLIC

transaction accepted from the user, except in respect of acts and omissions by the payee's payment service provider, who was selected solely by the payee. However, in order not to leave the payer unprotected in the unlikely circumstances that it is not clear that the payment amount was duly received by the payee's payment service provider, the corresponding burden of proof should lie on the payer's payment service provider. As a rule, it can be expected that the intermediary institution, usually an impartial body such as a central bank or a clearing house, that transfers the payment amount from the sending to the receiving payment service provider, will store the account data and will be able to provide the data where necessary. Where the payment amount has been credited to the receiving payment service provider's account, the payee should immediately have a claim against the payment service provider for credit of the account.			
(95) The payer's payment service provider, namely the account servicing payment service provider or, where appropriate, the payment initiation service			

PUBLIC

provider, should assume liability for correct payment execution, including the full amount of the payment transaction and execution time, and full responsibility for any failure by other parties in the payment chain up to the account of the payee. As a result of that liability, the payment service provider of the payer should, where the full amount is not credited or is only credited late to the payee's payment service provider, correct the payment transaction or without undue delay refund the payer the relevant amount of that transaction, without prejudice to any other claims which may be made in accordance with national law. Due to the payment service provider's liability, the payer or payee should not be burdened with any costs relating to an incorrect payment. In the case of non-execution, defective or late execution of payment transactions, the value date of corrective payments of payment service providers should always be the same as the value date in the case of correct execution.			
(96) The proper functioning of credit transfers and other payment services requires that payment service providers and their			

PUBLIC

intermediaries, including processors, have contracts in which their mutual rights and obligations are laid down. Questions relating to liabilities form an essential part of those contracts. To ensure mutual confidence among payment service providers and intermediaries taking part in a payment transaction, legal certainty is necessary to the effect that a non-responsible payment service provider is compensated for losses incurred or sums paid pursuant to the rules on liability. Further rights and details of content of recourse and how to handle claims towards the payment service provider or intermediary attributable to a defective payment transaction should be subject to agreement.			
(97) Provision of payment services by the payment services providers may entail the processing of personal data. The provision of account information services may entail the processing of personal data concerning a data subject who is not the user of a specific payment service provider, but whose personal data processing by that specific payment service provider is necessary for the performance of a contract between the			

PUBLIC

provider and the payment service user. Where personal data are processed, the processing should comply with Regulation (EU) 2016/679 and with Regulation (EU) 2018/1725 of the European Parliament and of the Council,[22] including the principles of purpose limitation, data minimisation and storage limitation. Data protection by design and data protection by default should be embedded in all data processing systems developed and used within the framework of this Regulation. Therefore, the supervisory authorities under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 should be responsible for the supervision of processing of personal data carried out in the context of this Regulation.			
(98) As acknowledged in the Communication from the Commission on a Retail Payments Strategy for the EU, the good functioning of EU payments markets is of substantial public interest. Therefore, when it is necessary in the context of this			

[22] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

PUBLIC

Regulation for the provision of payment services and for the compliance with this Regulation, payment service providers and payment system operators should be able to process special categories of personal data as defined in Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725. Where special categories of personal data are processed, payment service providers and payment system operators should implement appropriate technical and organisational measures to safeguard the fundamental rights and freedoms of natural persons. Those measures should include technical limitations on the re-use of data and the use of state-of-the-art security and privacy-preserving measures, including pseudonymisation, or encryption to ensure compliance with the principles of purpose limitation, data minimisation and storage limitation, as laid down in Regulation (EU) 2016/679. The payment service providers and payment systems should also implement specific organisation measures, including training on processing such data, limiting access to special categories of data and recording such access.			

PUBLIC

(99) The provision of information to individuals about the processing of personal data should be carried out in accordance with Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.			
(100) Fraudsters often target the most vulnerable individuals of our society. The timely detection of fraudulent payment transactions is essential, and transaction monitoring plays an import role in that detection. It is therefore appropriate to require payment service providers to have in place transaction monitoring mechanisms, reflecting the crucial contribution of those mechanisms to fraud prevention, going beyond the protection offered by strong customer authentication, in respect of payment transactions, including transactions involving payment initiation services.		(100) Fraudsters often target the most vulnerable individuals of our society. The timely detection of fraudulent payment transactions is essential, and transaction monitoring plays an import role in that detection. It is therefore appropriate to require both the payer's payment service provider and the payee's payment service provider~~s~~ to have in place transaction monitoring mechanisms, reflecting the crucial contribution of those mechanisms to fraud prevention, going beyond the protection offered by strong customer authentication, in	

		respect of payment transactions, including transactions involving payment initiation services. The payment service provider of the payer should carry out such transaction monitoring prior to the execution of a payment transaction, which means for instant credit transfers in real-time. ***[PRES comment:*** *The proposal presented at the January CWP meeting.]*	
(101) The EBA should develop draft regulatory technical standards on the specific technical requirements related to transaction monitoring mechanisms. Such requirements should build on the added value stemming from environmental and behavioural characteristics related to payment habits of the payment service user.			
(102) To ensure that transaction monitoring mechanisms work effectively to enable payment service providers to detect and	(102) Due to the complexity and the volume of fraudulent transactions, and to ensure that transaction monitoring mechanisms work	(102) Due to the complexity and the volume of fraudulent transactions, and to ensure that transaction monitoring	

prevent fraud, in particular by detecting atypical use of payment services that could indicate a potentially fraudulent transaction, payment service providers should be able to process information about their customers' transactions and their payment accounts. Payment service providers should, however, establish appropriate retention periods for different data types used for fraud prevention. Those retention periods should be strictly limited to the period necessary to detecting atypical, potentially fraudulent behaviour, and payment services providers should regularly delete the data that are not necessary anymore for fraud detection and prevention. Data processed for transaction monitoring purposes should not be used after the payment service user has ceased to be a customer of the payment service provider.	effectively to enable payment service providers to facilitate and prevent fraud detection in particular by detecting atypical use of payment services that could indicate a potentially fraudulent transaction, payment service providers should be able to process information about their customers' transactions and their payment accounts. Payment service providers should, however, establish appropriate retention periods for different data types used for fraud prevention. Those retention periods should be strictly limited to the period necessary to detecting atypical, potentially fraudulent behaviour, and payment ~~services~~ providers should regularly delete the data that are not necessary anymore for fraud detection and prevention. Data processed for transaction monitoring purposes should not be used after the payment service user has ceased to be a customer of the payment service provider.	mechanisms work effectively to enable payment service providers to facilitate and prevent fraud detection in particular by detecting atypical use of payment services that could indicate a potentially fraudulent transaction, payment service providers should be able to process information about their customers' transactions and their payment accounts. Payment service providers should, however, establish appropriate retention periods for different data types used for fraud prevention. Those retention periods should be strictly limited to the period necessary to detecting atypical, potentially fraudulent behaviour, and payment ~~services~~ providers should regularly delete the data that are not necessary anymore for fraud detection and prevention. Data	

	Transaction monitoring ~~of received payment transactions~~ by the payee's payment service provider, aimed at detecting suspicious fraud patterns, should be based on, inter alia, the amount, origin, frequency of those transactions with respect to the profile of the account holder as well as possible deviation of the payee's name in transaction against the payee's name held by the payment service provider of the payee.The transaction monitoring is also an obligation on the side of the payee's payment service provider, to accompany the proposed amendment in Art 83a. If the payer's payment service provider identifies a suspicious transaction, it shall execute that transaction. However, the level of monitoring should be based on risk-based approach and be based on precise and relevant criteria in line with the relevant data protection rules.	processed for transaction monitoring purposes should not be used after the payment service user has ceased to be a customer of the payment service provider. Transaction monitoring of received payment transactions ~~by the payee's payment service provider~~, aimed at detecting suspicious fraud patterns, should be based on, inter alia, the amount, origin, frequency of those transactions with respect to the profile of the account holder ~~as well as possible deviation of the payee's name in transactions against the payee's name held by the payment service provider of the payee.The transaction monitoring is also an obligation on the side of the payee's payment service provider, to accompany the proposed amendment in Art 83a.~~	

		~~If the payer's payment service provider identifies a suspicious transaction, it shall execute that transaction. However, the level of monitoring should be based on risk-based approach and be based on precise and relevant criteria in line with the relevant data protection rules.~~ ***[PRES comment:*** *The proposal presented at the January CWP meeting.]*	
(103) Fraud in credit transfers is inherently adaptive and comprises an open-ended diversity of practices and techniques, including the stealing of authentication credentials, invoice tampering, and social manipulation. Therefore, to be able to prevent ever new types of fraud, transaction monitoring should be constantly improved, making full use of technology such as artificial intelligence. Often one payment service provider does not have the full picture about all elements that could lead to timely	(103) Fraud in credit transfers is inherently adaptive and comprises an open-ended diversity of practices and techniques, including the stealing of authentication credentials, invoice tampering, and social manipulation. Therefore, to be able to prevent ever new types of fraud, transaction monitoring should be constantly improved, making full use of technology such as artificial intelligence. Often one payment		

PUBLIC

fraud detection. However, it can be made more effective with a greater amount of information on potentially fraudulent activity stemming from other payment service providers. Therefore, sharing of all relevant information between payment service providers should be possible. To better detect fraudulent payment transactions and protect their customers, payment services providers should, for the purpose of transaction monitoring, make use of payment fraud data shared by other payment services providers on a multilateral basis such as dedicated IT platforms based on information sharing arrangements. To improve the protection of payers against fraud in credit transfers, payment service providers should be able to rely on information as comprehensive and up to date as possible, namely by collectively using information concerning unique identifiers, manipulation techniques and other circumstances associated with fraudulent credit transfers identified individually by each payment services provider. Before concluding an information sharing arrangement, payment service providers should carry out a data protection	service provider does not have the full picture about all elements that could lead to timely fraud detection. However, it can be made more effective with a greater amount of information on potentially fraudulent activity stemming from other payment service providers. Therefore, sharing of all relevant information between payment service providers should be possible. To better detect fraudulent payment transactions and protect their customers, payment services providers should, for the purpose of transaction monitoring, make use of payment fraud data shared by other payment services providers on a multilateral basis such as dedicated IT platforms based on information sharing arrangements. To improve the protection of payers against fraud in credit transfers, payment service providers should be able to rely on information as comprehensive and up to date as possible, namely by collectively using information		

PUBLIC

impact assessment, in accordance with Article 35 of Regulation (EU) 2016/679. Where the data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons, payment service providers should consult the relevant data protection authority in accordance with Article 36 of that Regulation (EU) 2016/679. A new impact assessment should not be required when a payment service provider joins an existing information sharing arrangement for which a data protection impact assessment has already been carried out. The information sharing arrangement should lay down technical and organisational measures to protect personal data. It should lay down roles and responsibilities under data protection laws, including in case of joint controllers, of all payment service providers.	concerning fraudulent credit transfers identified individually by each payment service provider, including unique identifiers~~,~~ and name of the payee, session and device data including device ID, or manipulation techniques ~~and other circumstances associated with fraudulent credit transfers identified individually by each payment services provider~~. Before concluding an information sharing arrangement, payment service providers should carry out a data protection impact assessment, in accordance with Article 35 of Regulation (EU) 2016/679. Where the data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons, payment service providers should consult the relevant data protection authority in accordance with Article 36 of that Regulation (EU) 2016/679. A new impact		

PUBLIC

	assessment should not be required when a payment service provider joins an existing information sharing arrangement for which a data protection impact assessment has already been carried out. The information sharing arrangement should lay down technical and organisational measures to protect personal data. It should lay down roles and responsibilities under data protection laws, including in case of joint controllers, of all payment service providers.		
	(103a) Timely sharing of relevant fraud data amongst payment service providers to enhance their transaction monitoring mechanisms plays an important role in achieving the objective of timely detection and prevention of fraudulent payment transactions. In some cases, different data sharing frameworks under other relevant Union legislation may apply to the data being shared. To ensure legal certainty regarding the	(103a) Timely sharing of relevant fraud data amongst payment service providers to enhance their transaction monitoring mechanisms plays an important role in achieving the objective of timely detection and prevention of fraudulent payment transactions. In some cases, different data sharing frameworks under	

	conditions under which payment service providers can share fraud related information for the purpose of fraud prevention, the conditions under which such data sharing is allowed under this Regulation should be specified. Information sharing should be subject to robust safeguards relating to confidentiality, data protection and use of information. This should be without prejudice to the requirements under AMLR not to disclose that a suspicious transaction has been reported to the FIU or that an internal analysis into ML and TF is being carried out, and should not lead to jeopardizing an AML/CFT investigation.	other relevant Union legislation may apply to the data being shared. To ensure legal certainty regarding the conditions under which payment service providers can share fraud related information for the purpose of fraud prevention, also with the relevant national authorities, the conditions under which such data sharing is allowed under this Regulation should be specified. Information sharing should be subject to robust safeguards relating to confidentiality, data protection and use of information. This should be without prejudice to the requirements under AMLR not to disclose that a suspicious transaction has been reported to the FIU or that an internal analysis into ML and TF is being carried	

		out, and should not lead to jeopardizing an AML/CFT investigation. *[**PRES comment:** The proposal presented at the January CWP meeting.]*	
(104) For the purpose of exchanging personal data with other payment service providers who are subject to information sharing arrangements, 'unique identifier' should be understood as referring to 'IBAN' as defined in Article 2 point 15 of Regulation (EU) 260/2012.			
(105) To prevent legitimate exchanges of information on potentially fraudulent activity leading to unjustified 'de-risking' or withdrawal of payment account services to payment services users without explanation or recourse, it is appropriate to have safeguards in place. Payment fraud data shared under a multilateral information sharing arrangement that may entail the disclosure of personal data, including unique identifiers of payees potentially involved in fraud in credit transfers, should only be used by payment services providers for the			

PUBLIC

purpose of enhancing transaction monitoring. Additional safeguards should be put in place by payment services providers, such as contacting the customer if he or she is the payer of a credit transfer which can be assumed to be fraudulent, and further monitoring of an account, where the unique identifier shared as potentially fraudulent designates a customer of that payment service provider. Payment fraud data shared amongst payment services providers in the context of such arrangements should not constitute grounds for withdrawal of banking services without detailed investigation.			
(106) Payment fraud becomes increasingly sophisticated, with fraudsters using manipulative and impersonating techniques which are difficult for payment service users to detect without a sufficient level of awareness and information about fraud. Payment service providers can play an important role in reinforcing fraud prevention by regularly taking every necessary initiative to increase their payment service users' understanding and awareness about the risks and trends of payment fraud.			

PUBLIC

In particular, payment service providers should run proper awareness raising programmes and campaigns on fraud trends and risks addressed to customers and employees of payment service providers, with the aim of helping customers realise that they are victim of a fraud attempt. Payment service providers should give to their consumers, through various media, adapted information about fraud, giving them clear messages and warnings, helping them to react properly when exposed to potentially fraudulent situations. The EBA should develop guidelines about the different types of programmes to be developed by payment service providers on payment fraud risks, taking into account the ever-changing nature of fraud-related risks.			
(107) Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to			

PUBLIC

the maximum extent possible, the risk of fraud. In the area of fraud, the major innovation of Directive (EU) 2015/2366 was the introduction of Strong Customer Authentication (SCA). The Commission's evaluation of the implementation of Directive (EU) 2015/2366 concluded that strong customer authentication has already been highly successful in reducing fraud.			
(108) SCA should not be circumvented notably by any unjustified reliance on SCA exemptions. Clear definitions of Merchant Initiated Transactions (MITs) and of Mail Orders or Telephone Orders (MOTOs) should be introduced since these notions, which may be relied upon to justify non-application of SCA, are diversely understood and applied and are subject to abusive reliance. Regarding MITs, strong customer authentication should be applied at the set-up of the initial mandate, without the need to apply SCA for subsequent merchant-initiated payment transactions. Regarding MOTOs, only the initiation of payment transactions - not their execution - should be non-digital for a transaction to be considered as a MOTO	(108) SCA should not be circumvented notably by any unjustified reliance on SCA exemptions. Clear definitions of Merchant Initiated Transactions (MITs) and of Mail Orders or Telephone Orders (MOTOs) should be introduced since these notions, which may be relied upon to justify non-application of SCA, are diversely understood and applied and are subject to abusive reliance. Regarding MITs, strong customer authentication should be applied at the set-up of the initial mandate, without the need to apply SCA for subsequent merchant-initiated payment transactions. Regarding MOTOs, only the placement ~~initiation~~ of the payment order		

PUBLIC

and, therefore, not be covered by the obligation to apply SCA. However, payment transactions based on paper-based payment orders, mail orders or telephone orders placed by the payer should still entail security requirements and checks by the payment service provider of the payer allowing authentication of the payment transaction. SCA should also not be circumvented by practices including resorting to an acquirer established outside of the Union to escape the SCA requirements.	~~transactions~~ - not ~~their~~ its authentication or execution - should be non-digital for a transaction to be considered as a MOTO and, therefore, not be covered by the obligation to apply SCA. However, payment transactions based on paper-based payment orders, mail orders or telephone orders placed by the payer should still entail security requirements and checks by the payment service provider of the payer allowing authentication of the payment transaction. SCA should also not be circumvented by practices including resorting to an acquirer established outside of the Union to escape the SCA requirements. In this sense, a card-based payment could be considered a MOTO transaction if the placement of the payment order takes place in a non-electronic way, for example, when payment details are transmitted from the cardholder to a merchant via non electronic channels.		
(109) As the payment service provider that should apply strong customer authentication			

PUBLIC

is the payment service provider that issues the personalised security credentials, payment transactions that are not initiated by the payer but by the payee only should not be subject to strong customer authentication to the extent that those transactions are initiated without any interaction or involvement of the payer. The regulatory approach to MITs and direct debits, both being transactions initiated by the payee, should be aligned and benefit from the same consumer protection measures, including refunds.			
(110) To improve financial inclusion, and in line with Directive (EU) 2019/882 of the European Parliament and of the Council[23] on accessibility requirements for products and services, all payment service users, including persons with disabilities, older persons, persons with low digital skills and those who do not have access to digital devices such as smartphones, should benefit from the protection against fraud which is provided by SCA, in particular when it comes to the use	(110) To improve financial inclusion, and in line with Directive (EU) 2019/882 of the European Parliament and of the Council[24] on accessibility requirements for products and services, all payment service users, including persons with disabilities, older persons, persons with low digital skills and those who do not have access to digital devices such as smartphones, should benefit from the		

[23] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

[24] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

PUBLIC

of remote digital payment transactions and online access to payment accounts as fundamental financial services. With the introduction of SCA, certain consumers in the Union found it impossible to carry out online transactions because of their material incapability of performing SCA. Therefore, payment service providers should ensure that their customers can benefit from various methods to perform SCA which are adapted to their needs and situations. These methods should not depend on one single technology, device or mechanism, or on the possession of a smartphone.	protection against fraud which is provided by SCA, in particular when it comes to the use of remote digital payment transactions and online access to payment accounts as fundamental financial services. Vulnerable group of persons like persons with disabilities, older persons, people with low digital skills and those who do not have access to digital channels or payment instruments need to have access to these means. The payment service provider is dedicated to implement these measures in a manner that aligns with the specific circumstances in question. With the introduction of SCA, certain consumers in the Union found it impossible to carry out online transactions because of their material incapability of performing SCA. Therefore, payment service providers should ensure that their ~~customers~~ consumers can benefit from various methods to perform SCA which are adapted to their needs and situations. These methods should		

PUBLIC

	not depend on one single technology, device or mechanism, or on the possession of a smartphone.		
(111) European Digital Identity Wallets implemented under Regulation (EU) No 910/2014[25] of the European Parliament and of the Council, as amended by Regulation [XXX], are electronic identification means that offer identification and authentication tools for accessing financial services across borders, including payment services. The introduction of the European Digital Identity Wallet would further facilitate cross-border digital identification and authentication for secure digital payments and facilitate the development of a pan-European digital payments landscape.			
(112) Growth of electronic commerce and mobile payments should be accompanied by a generalised enhancement of security measures. In case of remote initiation of a payment transaction, i.e., when a payment order is placed via the internet, the authentication of transactions should rely on			

[25] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73–114).

PUBLIC

dynamic codes in order to make the user aware, at all times, of the amount and the payee of the transaction that the user is authorising.			
(113) The requirement to apply SCA for remote payment transactions through codes which dynamically link the transaction to a specific amount and a specific payee should reflect the growth of mobile payments and the emergence of a variety of models through which mobile payments are executed.			
(114) Given that dynamic linking addresses the risks of tampering with the payee name and the specific amount of the transaction between the moment a payment order is placed and authentication of payments, but also the risk of fraud more generally, for mobile payments for which the performance of strong customer authentication requires the use of internet on the payer's device, payment service providers should also apply elements which dynamically link the transaction to a specific amount and a specific payee or harmonised security measures of identical effect, which ensure the confidentiality, authenticity and integrity of			

PUBLIC

the transaction throughout all of the phases of initiation.			
(115) Under the exemption from SCA under Article 18 of Delegated Regulation (EU) 2018/389, payment service providers were allowed not to apply SCA where the payer initiated a remote electronic payment transaction identified by the payment service provider as posing a low level of risk evaluated on the basis of transaction monitoring mechanisms. Feedback from the market showed however that, in order to have more payment service providers implementing transaction risk analysis, it is necessary to adopt appropriate rules on the scope of transaction risk analysis, introducing clear audit requirements, providing more detail and better definitions on risk monitoring requirements and data to share, and to assess the potential benefits of allowing payment service providers to report fraudulent transactions for which they are solely liable. The EBA should develop draft Regulatory Technical Standards laying down rules on transaction risk analysis.			

PUBLIC

(116) Security measures should be compatible with the level of risk involved in payment services. To allow the development of user-friendly and accessible means of payment for low-risk payments, such as low value contactless payments at the point of sale, whether or not these payments are based on mobile phone, the exemptions to the application of security requirements should be specified in regulatory technical standards. Safe use of personalised security credentials is needed to limit the risks relating to spoofing, phishing and other fraudulent activities. The user should be able to rely on the adoption of measures that protect the confidentiality and integrity of personalised security credentials.			
(117) Payment service providers should apply SCA when, *inter alia*, the payment service user is carrying out any action through a remote channel which may imply the risk of payment fraud or other abuses. Payment service providers should have in place adequate security measures to protect the confidentially and integrity of the			

PUBLIC

payment service user´s personalised security credentials.			
(118) There is no consistent understanding by market stakeholders across Member States of the SCA requirements applicable to the enrolment of payment instruments, in particular payment cards, in digital wallets. The creation of a token or its replacement process may give rise to a risk of payment fraud or other abuses. The creation or replacement of a token of a payment instrument, which is done via a remote channel with the participation of the payment service user, should therefore require application of SCA by the payment service provider of the payment service user at the time of the issuance or replacement of the token. By applying SCA at the token creation or replacement stage, the payment service provider should verify remotely that the payment service user is the rightful user of the payment instrument and associate the user and the digitised version of the payment instrument with the respective device.			
(119) Operators of digital pass-through wallets that verify the elements of SCA when			

PUBLIC

tokenised instruments stored in the digital wallets are used for payments should be required to enter into outsourcing agreements with the payers' payment service providers to allow them to continue to perform such verifications, but also requiring them to comply with key security requirements. The payer's payment service providers should, under such agreements, retain full liability for any failure by operators of digital pass-through wallets to apply SCA and have the right to audit and control the wallet operator's security provisions.			
(120) Where technical service providers or operators of payment schemes provide services to payees or to the payment service providers of payees or of payers, they should support the application of strong customer authentication within the remit of their role in the initiation or execution of payment transactions. Given the role that they play in ensuring that key security requirements concerning retail payments are properly implemented, including by providing appropriate IT solutions, technical service providers and operators of payment schemes			

PUBLIC

should be held liable for the financial damages caused to payees or to the payment service providers of the payees or of the payers in case they fail to support the application of strong customer authentication.			
(121) Member States should designate the competent authorities for granting authorisation to payment institutions and for accreditation and monitoring of alternative dispute resolution (ADR) procedures.			
		(121a) To ensure that an undertaking does not provide payment services without being authorised, it is appropriate to require all undertakings intending to provide payment services to apply for an authorisation, except where Directive (EU) XXX (PSD3) provides for registration instead of authorisation. Furthermore, in order to ensure the stability and integrity of the financial system and payment systems	

		and to protect consumers, such undertakings must be established in a Member State and effectively supervised. *[**PRES comment**: Recital for Article 89a PSR.]*	
		(121b) Competent authorities should be conferred with effective powers to investigate unauthorised payments services and to enforce the authorization requirement, to supervise the provision of payment services as well as to supervise payment service providers. Over and above that, the unauthorised provision of payment services shall constitute a criminal offence in the respective Member States which shall as felony be tried before and punished by a criminal court.	

		*[**PRES comment**: Similar to Recital 98 MiCAR. See the amendments to Article 91(3).]*	
		(121c) Those powers bestowed upon the supervisory authorities should include the power to intervene against unauthorised payment services, including the power to investigate alleged infringements - in particular of the authorisation requirement -, to order the immediate cessation of business operations and the immediate full settlement of already concluded activities, and to investigate infringements of the rules on this Regulation and Directive (EU) XXX (PSD3). To enable competent authorities to effectivly enforce the authorisation requirement	

PUBLIC

		and to properly supervise payment institutions, it is appropriate to grant those authorities investigatory and supervisory powers and the possibility to impose administrative penalties and measures necessary to perform their tasks. For the same reason, it is appropriate to grant competent authorities the power to request information, conduct on-site inspections, search business premises as well as private home estate, ancillary facilities, movables and persons. It should have the authoritiy to issue recommendations, guidelines and binding administrative decisions. Member States should empower their competent authorities to impose administrative sanctions and measures aimed specifically at ending	

		infringements of provisions concerning the supervision or pursuit of the payment service business. *[**PRES comment**: Similar to Recital 98 MiCAR and Recital 49 PSD3. See the amendments to Article 91(3).]*	
		(121d) Furthermore, it is necessary that the competent authorities have the powers mutatis mutandis to take action against third parties involved in the initiation, conclusion or processing of unauthorised payment services. In particular, there should be powers to request information from providers of intermediary services within the meaning of Regulation (EU) 2022/2065 that contribute to the operation of unauthorised payment services and to	

PUBLIC

		instruct them to block or restrict access to websites hosted by operators of unauthorised payment services. In the interest of temporarily safeguarding customer funds and other assets, these powers should already take effect at the investigation stage if there is a reasonable suspicion (facts justifying the assumption) of unauthorised business operations. ***[PRES comment**: See the amendments to Article 91(3).]*	
(122) Without prejudice to the right of customers to bring action in courts, Member States should ensure the existence of easily accessible, adequate, independent, impartial, transparent and effective ADR procedures between payment service providers and payment service users. Regulation (EC) No 593/2008 of the European Parliament and of	(122) Without prejudice to the right of customers to bring action in courts Member States should ensure the existence of easily accessible, adequate, independent, impartial, transparent and effective ADR procedures between payment service providers and payment service users. ~~To ensure a high level of consumer~~	(122) Without prejudice to the right of customers to bring action in courts Member States should ensure the existence of easily accessible, adequate, independent, impartial, transparent and effective ADR procedures between	

the Council[26] provides that the protection afforded to consumers by the mandatory rules of the law of the country in which they have their habitual residence is not to be undermined by any contractual terms concerning the law applicable to the contract. With a view to establishing an efficient and effective dispute resolution procedure, Member States should ensure that payment service providers subscribe to an ADR procedure in compliance with the quality requirements laid down in Directive 2013/11/EU of the European Parliament and of the Council[27], to resolve disputes before resorting to a court. Designated competent authorities should notify the Commission of a competent quality ADR entity or entities on their territory to resolve national and cross-border disputes and to cooperate with regard to disputes concerning rights and obligations pursuant to this Regulation.	~~protection, payment service providers should be required to participate in ADR procedures at the request of payment service users who are consumers, regarding all disputed payment transactions.~~ Regulation (EC) No 593/2008 of the European Parliament and of the Council provides that the protection afforded to consumers by the mandatory rules of the law of the country in which they have their habitual residence is not to be undermined by any contractual terms concerning the law applicable to the contract. ~~The possibility to seek judicial redress in accordance with the laws of the Member State concerned, and therefore should not affect the exercise of the right to an effective judicial remedy under Article 47 of the Charter of Fundamental Rights of the European Union.~~ With a view to	payment service providers and payment service users. ~~To ensure a high level of consumer protection, payment service providers should be required to participate in ADR procedures at the request of payment service users who are consumers, regarding all disputed payment transactions.~~ Regulation (EC) No 593/2008 of the European Parliament and of the Council provides that the protection afforded to consumers by the mandatory rules of the law of the country in which they have their habitual residence is not to be undermined by any contractual terms concerning the law applicable to the	

[26] OJ L 177, 4.7.2008, p. 6–16.
[27] Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (OJ L 165, 18.6.2013, p. 63–79).

PUBLIC

	establishing an efficient and effective dispute resolution procedure, Member States should ensure that payment service providers subscribe to an ADR procedure in compliance with the quality requirements laid down in Directive 2013/11/EU of the European Parliament and of the Council54, to resolve disputes before resorting to a court. Designated competent authorities should notify the Commission of a competent quality ADR entity or entities on their territory to resolve national and cross-border disputes and to cooperate with regard to disputes concerning rights and obligations pursuant to this Regulation. For contractual consumer-to-business disputes regarding the purchase of goods or services, Directive 2013/11/EU ensures that Union consumers and businesses in the Union have access to quality-certified out-of-court dispute resolution entities. In this regard, it should be clarified that the rules of this	contract. ~~The possibility to seek judicial redress in accordance with the laws of the Member State concerned, and therefore should not affect the exercise of the right to an effective judicial remedy under Article 47 of the Charter of Fundamental Rights of the European Union.~~ With a view to establishing an efficient and effective dispute resolution procedure, Member States should ensure that payment service providers subscribe to an ADR procedure in compliance with the quality requirements laid down in Directive 2013/11/EU of the European Parliament and of the Council54, to resolve disputes before resorting to a court. Designated competent authorities should notify the Commission of a competent quality ADR entity or entities	

PUBLIC

	Regulation on out-of-court dispute settlement are without prejudice to Directive 2013/11/EU.	on their territory to resolve national and cross-border disputes and to cooperate with regard to disputes concerning rights and obligations pursuant to this Regulation. For contractual consumer-to-business disputes regarding the purchase of goods or services, Directive 2013/11/EU ensures that Union consumers and businesses in the Union have access to ADR quality-certified out-of-court dispute resolution entities that comply with the quality requirements set out in the ~~. In this regard, it should be clarified that the rules of this Regulation on out-of-court dispute settlement are without prejudice to~~ Directive 2013/11/EU. ***[PRES comment:*** *Wording aligned with the ADR*	

PUBLIC

		Directive 2013/11/EU, as requested by one of the Member States.]	
(123) Consumers should be entitled to enforce their rights in relation to the obligations imposed on payment and electronic money service providers under this Regulation through representative actions in accordance with Directive (EU) 2020/1828 of the European Parliament and of the Council'[28].			
(124) Appropriate procedures should be established to pursue complaints against payment service providers which do not comply with their obligations and to ensure that, where appropriate, effective, proportionate and dissuasive penalties are imposed. To ensure effective compliance with this Regulation, Member States should designate competent authorities which meet the conditions laid down in Regulation (EU) No 1093/2010 of the European Parliament and of the Council[29] and which act			

[28] Directive (EU) 2020/1828 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, (OJ L 409, 4.12.2020, pp. 1–27).

[29] 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).

PUBLIC

independently from the payment service providers. Member States should notify the Commission which authorities have been designated, with a clear description of their tasks.			
(125) Without prejudice to the right to bring action in court to ensure compliance with this Regulation, competent authorities should exercise the necessary powers granted under this Regulation, including the power to investigate alleged infringements and to impose administrative sanctions and administrative measures, where the payment service provider does not comply with the rights and obligations laid down in this Regulation, in particular if there is a risk of re-offending or another concern for collective consumer interests. Competent authorities should establish effective mechanisms to encourage reporting of potential or actual breaches. Those mechanisms should be without prejudice to the rights of the defense of anyone who has been charged.			
(126) Member States should be required to provide for effective, proportionate and			

PUBLIC

dissuasive administrative sanctions and administrative measures in relation to infringements of provisions from this Regulation. Those administrative sanctions, periodic penalty payments and administrative measures should meet certain minimum requirements, including the minimum powers that should be vested on competent authorities to be able to impose them, the criteria that competent authorities should take into account in their application in their publication and in reporting about them. Member States should lay down specific rules and effective mechanisms regarding the application of periodic penalty payments.			
(127) Competent authorities should be empowered to impose administrative pecuniary penalties which are sufficiently high to offset the benefits that can be expected and to be dissuasive even to larger institutions.			
(128) When imposing administrative sanctions and measures, competent authorities should have regard to any previous criminal penalties that may have			

PUBLIC

been imposed on the same natural or legal person responsible for the same breach when determining the type of administrative penalties or other administrative measures and the level of administrative pecuniary penalties. This is to ensure that the severity of all the penalties and other administrative measures imposed for punitive purposes in case of duplication of administrative and criminal proceedings is limited to what is necessary in the view of the seriousness of the breach concerned.			
(129) An effective supervisory system requires that supervisors are aware of the weaknesses in payment services providers' compliance with rules in this Regulation. It is therefore important that supervisors be able to inform one another of administrative sanctions and measures imposed on payment services providers, when such information would be relevant for other supervisors too.			
(130) The effectiveness of the Union framework for payment services depends on cooperation between a wide array of competent authorities, including national authorities responsible for taxation, data			

PUBLIC

protection, competition, consumer protection, audit, police and other enforcement authorities. Member States should ensure that their legal framework allows and facilitates such cooperation as required, to achieve the goals of the Union framework for payment services also through the proper enforcement of its rules. Such cooperation should include exchange of information as well as mutual assistance for effective enforcement of administrative sanctions, in particular in the cross-border recovery of pecuniary penalties.			
(131) Irrespective of their denomination under national law, forms of expedited enforcement procedure or settlement agreements can be found in many Member States and are used as an alternative to formal proceedings to achieve a swifter adoption of a decision aiming at imposing an administrative sanction or administrative measure or to put an end to the alleged breach and its consequences before formal sanctioning proceedings are started. While it does not appear appropriate to strive to harmonize at Union level such enforcement			

PUBLIC

methods introduced by many Member States, due to the very varied legal approaches adopted at national level, it should be acknowledged that such methods allow competent authorities that can apply them to handle infringement cases in a speedier, less costly and overall efficient way under certain circumstances, and should therefore be encouraged. However, Member States should not be under the obligation to introduce such enforcement methods in their legal framework nor to compel competent authorities to use them if they do not deem it appropriate.			
(132) Member States have established and currently provide for a diverse range of administrative sanctions and administrative measures for breaches of the key provisions regulating the provisions of payment services and inconsistent approaches to investigating and sanctioning violations of those provisions. Failing to set out more clearly what core provisions must trigger sufficiently dissuasive enforcement everywhere in the Union would thwart the achievement of the single market for			

PUBLIC

payment services and would risk incentivising forum shopping insofar as competent authorities are unevenly equipped to enforce promptly and with the same deterrence these infringements in the Member States.			
(133) Since the purpose of the periodic penalty payments is to compel natural or legal persons who are identified as responsible for an ongoing infringement or are required to comply with an order from the investigating competent authority, to comply with that order or terminate the ongoing breach, the application of periodic penalty payments should not prevent competent authorities from imposing subsequent administrative sanctions for the same infringement.			
(134) Unless otherwise provided for by Member States, periodic penalty payments should be calculated on a daily basis.			
(135) Competent authorities should be empowered by Member States to impose such administrative sanctions and administrative measures on payment services providers or other natural or legal persons			

PUBLIC

where relevant to remedy the situation in the case of infringement. The range of sanctions and measures should be sufficiently broad to allow Member States and competent authorities to take account of the differences between payment service providers, in particular between credit institutions and other payment institutions, as regards their size, characteristics and the nature of the business.			
(136) The publication of an administrative sanction or measure for infringement of provisions of this Regulation can have a strong dissuasive effect against repetition of such infringement. Publication also informs other entities of the risks associated with the sanctioned payment services provider before entering into a business relationship and assists competent authorities in other Member States in relation to the risks associated with a payment services provider when it operates in their Member States on a cross-border basis. For those reasons, the publication of decisions on administrative sanctions and administrative measures should be allowed as long as it concerns legal	(136) The publication of an administrative sanction or measure for infringement of provisions of this Regulation can have a strong dissuasive effect against repetition of such infringement. Publication also informs other entities of the risks associated with the sanctioned payment services provider before entering into a business relationship and assists competent authorities in other Member States in relation to the risks associated with a payment services provider when it operates in their Member States on a cross-border basis. For those reasons, the		

PUBLIC

persons. In taking a decision whether to publish an administrative sanction or administrative measure, competent authorities should take into account the gravity of the infringement and the dissuasive effect that the publication is likely to produce. However, any such publication referred to natural persons may impinge on their rights stemming from the Charter of Fundamental Rights and the applicable Union data protection legislation in a disproportionate manner. Therefore, publication should occur in an anonymised way unless the competent authority deems it necessary to publish decisions containing personal data for the effective enforcement of this Regulation, including in the case of public statements or temporary bans. In such cases the competent authority should justify its decision.	publication of decisions on administrative sanctions and administrative measures, and also the right of appeal against these publications should be allowed as long as it concerns legal persons. In taking a decision whether to publish an administrative sanction or administrative measure, competent authorities should take into account the gravity of the infringement and the dissuasive effect that the publication is likely to produce. However, any such publication referred to natural persons may impinge on their rights stemming from the Charter of Fundamental Rights and the applicable Union data protection legislation in a disproportionate manner. Therefore, publication should occur in an anonymised way unless the competent authority deems it necessary to publish decisions containing personal data for the effective enforcement of this Regulation, including in the case of		

PUBLIC

	public statements or temporary bans. In such cases the competent authority should justify its decision.		
(137) To collect more accurate information on the level of compliance with Union law on the ground, while giving competent authorities' enforcement activity more visibility, it is necessary to enlarge the scope and improve the quality of the data that competent authorities report to the EBA. Information to be reported should be anonymised to comply with data protection rules in force and provided in aggregated form to comply with professional secrecy and confidentiality rules as regards proceedings. The EBA should report regularly to the Commission on the progress of enforcement actions in the Member States.			
(138) The power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission to update, to take account of inflation, the amounts up to which a payer may be obliged to bear the losses relating to any unauthorised payment transactions resulting from the use			

PUBLIC

of a lost or stolen payment instrument or from the misappropriation of a payment instrument. The Commission, when preparing delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.			
(139) In order to ensure consistent application of this Regulation, the Commission should be able to rely on the expertise and support of the EBA, which should have the task of preparing guidelines and draft Regulatory and Implementing Technical Standards. The Commission should be empowered to adopt those draft Regulatory Technical Standards. The EBA should, when developing guidelines, draft Regulatory Technical Standards and draft Implementing Technical Standards pursuant to this Regulation and in accordance with Regulation (EU) No 1093/2010, consult all relevant stakeholders, including those in the payment services market, reflecting all interests involved.			
(140) The EBA should, in line with Article 9(5) of Regulation (EU) No 1093/2010, be			

PUBLIC

granted product intervention powers to be able to temporarily prohibit or restrict in the Union certain type or a specific feature of a payment service or an electronic money service which is identified as potentially causing harm to consumers, threatening the orderly functioning and integrity of financial markets. Regulation (EU) No 1093/2010 should therefore be amended accordingly.			
(141) The Annex to Regulation (EU) 2017/2394 of the European Parliament and of the Council[30] should be amended to include a reference to this Regulation to facilitate cross-border cooperation on the enforcement of this Regulation.			
(142) Since the objective of this Regulation, namely further integration of an internal market in payment services, cannot be sufficiently achieved by the Member States because it requires harmonisation of various different rules in Union and national law, but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance			

[30] Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/200 (OJ L 345, 27.12.2017, p. 1–26).

PUBLIC

with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.			
(143) Considering that this Regulation and Directive (EU) XXX (PSD3) lay down the legal framework governing the provision of retail payment services and electronic money services within the Union, to ensure legal certainty and consistency of the Union's legal framework, this Regulation should apply from the same date as the date of application of the laws, regulations and administrative provisions that Member States are required to adopt to comply with Directive (EU) XXX (PSD3). However, the provisions requiring payment service providers to verify discrepancies between the name and unique identifier of a payee in case of credit transfers and the respective liability regime should apply from 24 months after the date of entry into force of this Regulation, thus granting payment service providers enough time to take the necessary steps to			

PUBLIC

adjust their internal systems, to comply with such requirements.			
(144) In keeping with the principles of better regulation, this Regulation should be reviewed for its effectiveness and efficiency in achieving its objectives. The review should take place a sufficient time after the date of application of this Regulation for adequate evidence to exist on which the review can be based. Five years is considered to be an appropriate period. While the review should consider this Regulation as a whole, certain topics should be singled out for particular attention, namely the functioning of open banking, the charging for payment services and further solutions to combat fraud. Regarding the scope of this Regulation, however, it is appropriate for a review to take place earlier, three years after entry into application, given the importance attached to that subject in Article 58(2) of Regulation (EU) 2022/2554 of the European Parliament and of the Council[31]. That review of scope should consider both the possible			

[31] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

PUBLIC

extension of the list of covered payment services to include services such as those performed by payment systems and payment schemes, and the possible inclusion in the scope of some technical services currently excluded.			
		(144a) In view of the increasing relevance of virtual IBANs, the Commission should review the impact of the newly adopted provisions contained in Regulation (EU) 2024/1624 and Directive (EU) 2024/1640 in relation to virtual IBANs. The review should take place a sufficient time after the entry into force of the above-mentioned legislations. The Commission's report based on this review should, in particular, assess the risks and challenges posed by virtual IBANs on the one hand, and their benefits on	

		the other one. On the grounds of this assessment, the Commission should conclude in its report, whether it is necessary to introduce any further measures regulating virtual IBANs at EU level and, if appropriate, submit a legislative proposal together with the report. ***[PRES comment:*** *The proposal presented at the January CWP meeting.]*	
(145) This Regulation respects fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, including the right to respect for private and family life, the right to protection of personal data, the freedom to conduct a business, the right to an effective remedy and the right not to be tried or punished twice in criminal proceedings for the same offence. This Regulation must be applied in accordance with those rights and principles.			

(146) References to amounts in euro, are to be understood as the national currency equivalent as determined by each non-euro Member State.		(146) References to amounts in euro, are to be understood as the national currency equivalent as determined by each non-euro Member State. References to payment transactions in euro or other currencies are to be understood as payment transactions with funds denominated in euro or other currencies, including electronic money tokens denominated in euro or other currencies. *[**PRES comment:** The proposal presented at the February CWP meeting.]*	
(147) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the			

PUBLIC

Council[32] and delivered an opinion on [XX XX 2023][33],			
HAVE ADOPTED THIS REGULATION:			
TITLE I			
SUBJECT MATTER, SCOPE AND DEFINITIONS			
Article 1			
Subject matter			
1. This Regulation lays down uniform requirements on the provision of payment services and electronic money services, as regards:			
(a) the transparency of conditions and information requirements for payment services and electronic money services;			
(b) the respective rights and obligations of payment and electronic money service users, and of payment and electronic money service providers in relation to the provision			

[32] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance.), (OJ L 295, 21.11.2018, p. 39–98).

[33] OJ C […], […], p. […].

PUBLIC

of payment services and electronic money services.			
2. Unless specified otherwise, any reference to payment services shall be understood in this Regulation as meaning payment and electronic money services.			
3. Unless specified otherwise, any reference to payment service providers shall be understood in this Regulation as meaning payment service providers and electronic money service providers.			
Article 2			
Scope			
1. This Regulation applies to payment services provided within the Union by the following categories of payment service providers:			
(a) credit institutions as defined in Article 4(1), point (1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council[34], including branches thereof where such branches are located in the Union, whether the head offices of those are			

[34] Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

PUBLIC

located within the Union or outside the Union;			
(b) post office giro institutions which are entitled under national law to provide payment services;			
(c) payment institutions;			
(d) the ECB and national central banks when not acting in their capacity as monetary authority or other public authorities;			
(e) Member States or their regional or local authorities when not acting in their capacity as public authorities.			
	1bis. This Regulation also applies to services provided within the Union by the following entities:		
	(a) technical service providers, for the purposes of Articles 23(2), 58, 87, 89, 91, and 93;		
	(b) operators of payment systems and payment schemes, for the purposes of Articles 31, 58, 80, 91 and 93;		
	(c) providers of electronic communications services, for the purposes of Articles 59, 91 and 93.		

2. This Regulation does not apply to the following services:		2. This Regulation does not apply to the following ~~services~~: ***[PRES comment:*** *The proposal presented at the February CWP meeting.]*	
(a) payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention;			
		a1) payment transactions with electronic money tokens, without any intermediary involved, including transfers of electronic money tokens between two self-hosted addresses; ***[PRES comment:*** *The proposal presented at the February CWP meeting.]*	
(b) payment transactions from the payer to the payee through a commercial agent, as defined in Article 1(2) of Directive 86/653/EEC, provided that all of following conditions are met : i) the commercial agent	(b) payment transactions from the payer to the payee through a commercial agent, ~~as defined in Article 1(2) of Directive 86/653/EEC~~, provided that all of		

PUBLIC

is authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee, but not both of them, irrespective of whether or not the commercial agent is in the possession of the client's funds, and ii) such agreement gives the payer or the payee a real margin to negotiate with the commercial agent or conclude the sale or purchase of goods or services;	following conditions are met: i) the commercial agent is authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee, but not both of them, ~~irrespective of whether or not the commercial agent is in the possession of the client's funds~~, and ii) such agreement gives the payer or the payee a real scope ~~margin~~ to negotiate with the commercial agent or conclude the sale or purchase of goods or services;		
	(b´) professional physical transport of banknotes and coins, including their collection, processing and delivery (cash-in-transit);	~~(b´) professional physical transport of banknotes and coins, including their collection, processing and delivery (cash-in-transit);~~ ***[PRES comment:*** *Identical provision is already included in let. n) of this paragraph.]*	
(c) payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity;			

(d) services where cash is provided by the payee to the payer as part of a payment transaction for the purchase of goods and services, following an explicit request by the payment service user just before the execution of the payment transaction;	~~(d) services where cash is provided by the payee to the payer as part of a payment transaction for the purchase of goods and services, following an explicit request by the payment service user just before the execution of the payment transaction. The payment service user shall be provided with information on any possible charges for this service before the requested cash is provided;~~	(d) services where cash is provided by the payee to the payer as part of a payment transaction for the purchase of goods and services, following an explicit request by the payment service user just before the execution of the payment transaction. The payment service user shall be provided with information on any possible charges for this service before the requested cash is provided; ***[PRES comment:*** *The reversion to this exemption results from the Member States' comments on the importance to keep it in the regulation.]*	
(e) services where cash is provided in retail stores following an explicit request by the payment service user but independently of the execution of any payment transaction and without any obligation to make a purchase of goods and services. The payment			

PUBLIC

service user shall be provided with information on any possible charges for this service before the requested cash is provided;			
	(e´) cash-to-cash currency exchange operations where the funds are not held on a payment account;	~~(e´) cash-to-cash currency exchange operations where the funds are not held on a payment account;~~ ***[PRES comment:*** *Identical provision is already included in let. o) of this paragraph.]*	
(f) payment transactions based on any of the following documents drawn on the payment service provider to place funds at the disposal of the payee:			
(i) paper cheques governed by the Geneva Convention of 19 March 1931 providing a uniform law for cheques;			
(ii) paper cheques similar to those referred to in point (i) and governed by the laws of Member States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques;			
(iii) paper-based drafts referred to in the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;			

PUBLIC

(iv) paper-based drafts similar to those referred to in point (iii) and governed by the laws of Member States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;			
(v) paper-based vouchers;		(v) paper-based vouchers or vouchers of similar nature; *[**PRES comment:** Based on the comment of one Member State stating that vouchers are not always paper-based, they can be electronic (in apps) or plastic based.]*	
(vi) paper-based traveller's cheques;			
(vii) paper-based postal money orders as defined by the Universal Postal Union;			
(g) payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses or central banks and other participants of the system, and payment service providers, without prejudice to Article 31;			
(h) payment transactions related to securities asset servicing, including			

PUBLIC

dividends, income or other distributions, or redemption or sale, carried out by persons as referred to in point (g) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments;			
		h1) payments transactions carried out by a crypto-asset service provider where electronic money tokens are exchanged for funds or crypto-assets; *[**PRES comment:** The proposal presented at the February CWP meeting.]*	
(i) without prejudice to Article 23(2), and Articles 58 and 87, services provided by technical service providers;	~~(i) without prejudice to Article 23(2), and Articles 58 and 87, services provided by technical service providers;~~		
(j) services based on specific payment instruments that meet one of the following conditions:			

PUBLIC

(i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a single limited network of service providers under direct commercial agreement with a professional issuer;			
(ii) instruments which can be used only to acquire a very limited range of goods or services;	(ii) instruments which can be used only to acquire a very limited range of goods or services, <u>including instruments restricted to be used in business-to-business transactions;</u>		
(iii) instruments valid only in a single Member State, which are provided at the request of an undertaking or a public sector entity and regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer;			
(k) payment transactions by a provider of electronic communications networks as defined in Article 2, point (1), of Directive (EU) 2018/1972 of the European Parliament and of the Council[35], or services provided in addition to electronic communications	(k) payment transactions by a provider of electronic communications networks as defined in Article 2, point (1), of Directive (EU) 2018/1972 ~~of the European Parliament and of the Council~~, or		

[35] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).

PUBLIC

services as defined in Article 2, point (4), of that Directive to a subscriber to the network or service:	services provided in addition to electronic communications services as defined in Article 2, point (4), of that Directive to a subscriber to the network or service:		
(i) to purchase digital content and voice-based services, regardless of the device used for the purchase or consumption of the digital content and charged to the related bill; or			
(ii) performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets;			
provided that the value of any single payment transaction does not exceed EUR 50 and:			
– the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month, or			
– where a subscriber pre-funds its account with the provider of the electronic communications network or service, the cumulative value of payment transactions does not exceed EUR 300 per month;			
(l) payment transactions carried out between payment service providers, their agents or branches for their own account;			

		(l1) payment transactions carried out between crypto-asset service providers or their branches for their own account; ***[PRES comment:*** *The proposal presented at the February CWP meeting.]*	
(m) payment transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group, and the collection of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission to a payment service provider.	(l ~~m~~) payment transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group, as well as the execution ~~and the collection~~ of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission and processing to a payment service provider, and the collection of funds from external third parties on behalf of group entities by a parent undertaking or its subsidiary.	(~~l~~ m) payment transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group, as well as the execution ~~and the collection~~ of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission and processing to a payment service provider, and the	

		collection of funds from external third parties on behalf of group entities by a parent undertaking or its subsidiary.	
	(m ~~n~~) professional physical transport of banknotes and coins, including their collection, processing and delivery (cash-in-transit);	(~~m~~ n) professional physical transport of banknotes and coins, including their collection, processing and delivery (cash-in-transit);	
	(n ~~o~~) cash-to-cash currency exchange operations where the funds are not held on a payment account.	(~~n~~ o) cash-to-cash currency exchange operations where the funds are not held on a payment account.	
3. Titles II and III apply to payment transactions in the currency of a Member State 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 within the Union.			
4. Title II, except for Article 13(1), point (b) , Article 20, point (2)(e) and Article 24, point (a), and Title III, except for Articles 67 to 72, apply to payment transactions in a currency that is not the currency of a Member	4. Title II, except for Article 13(1), point (b) , Article 20, ~~point (2)(e)~~ b) v) and Article 24, point (a), and Title III, except for Articles 67 to 72, apply to payment transactions in a currency		

PUBLIC

State, 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 within the Union, in respect to those parts of the payments transaction which are carried out in the Union.	that is not the currency of a Member State, 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 within the Union, in respect to those parts of the payments transaction which are carried out in the Union.		
5. Title II, except for Article 13(1), point (b), Article 20, point (2)(e) and point (5)(h) and Article 24, point (a), and Title III, except for Article 28(2) and (3), Articles 62, 63 and 67, Article 69(1), and Articles 75 and 78, apply to payment transactions in all currencies 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.	5. Title II, except for Article 13(1), point (b), Article 20, ~~point (2)(e)~~ b) v) and point ~~(5)(h)~~ e) viii) and Article 24, point (a), and Title III, except for Article 28(2) and (3), Articles 62, 63 and 67, Article 69(1), and Articles 75 and 78, apply to payment transactions in all currencies 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.		
6. Member States may exempt institutions referred to in Article 2(5), points (4) to (23), of Directive 2013/36/EU from the			

PUBLIC

application of all or part of the provisions of this Regulation.			
7. By [OP please insert the date= one year after the date of entry into force of this Regulation], the EBA shall issue Guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010, addressed to the competent authorities designated under this Regulation, on the exclusion for payment transactions from the payer to the payee through a commercial agent referred to in paragraph 2, point (b) of this Article.			
8. The EBA shall develop draft Regulatory Technical Standards to specify the conditions of the exclusions referred to in paragraph 2, point (j). The EBA shall take into account the experience acquired in the application of the EBA guidelines of 24 February 2022 on the limited network exclusion under Directive (EU) 2015/2366.			
The EBA shall submit the Regulatory Technical Standards referred to in the first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated on the Commission to adopt the			

PUBLIC

Regulatory Technical Standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.			
9. Member States shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 6, by the date of application of this Regulation, and, without delay, any subsequent amendment affecting them.			
Article 3			
Definitions			
For the purposes of this Regulation, the following definitions apply:			
(1) 'home Member State' means either of the following:			
(a) the Member State in which the payment service provider has its registered office; or			
(b) if the payment service provider has, under its national law, no registered office, the Member State in which the payment service provider has its head office;			

(2) 'host Member State' means the Member State other than the home Member State in which a payment service provider has an agent, a distributor or a branch or provides payment services;		(2) 'host Member State' means the Member State other than the home Member State in which a payment service provider has an agent~~,~~ ~~a distributor~~ or a branch or provides payment services; *[**PRES comment**: The consequence of the approach taken by the Member States in the Council to delete the notion of distributors.]*	
(3) 'payment service' means any business activity set out in Annex I;	(3) 'payment service' means any business activity set out in points 1 to 7 of the Annex I	(3) 'payment service' means any business activity set out in points 1 to 7 of the Annex I to Directive XXX [PSD3]; *[**PRES comment**: The alignment with the approach taken under the Hungarian Presidency to remove Annex I from the PSR and maintain the Annex on payment services only in PSD3.]*	
(4) 'payment institution' means a legal person that has been granted authorisation in accordance with Article 13 of Directive (EU)	(4) 'payment institution' ~~means a legal person that has been granted authorisation in accordance with~~		

PUBLIC

[PSD3] to provide payment services or electronic money services throughout the Union;	~~Article 13 of Directive (EU) [PSD3] to provide payment services or electronic money services throughout the Union;~~ means a payment institution as defined in Article 2 point (4) of Directive XXX [PSD3];		
(5) 'payment transaction' means an act of placing, transferring or withdrawing funds, based on a payment order placed by the payer, or on his behalf, or by the payee, or on his behalf, irrespective of any underlying obligations between the payer and the payee;			
(6) 'initiation of a payment transaction' means the steps necessary to prepare the execution of a payment transaction, including the placement of a payment order and the completion of the authentication process;			
(7) 'remote initiation of a payment transaction' means a payment transaction for which a payment order is placed via the internet;			
(8) 'execution of a payment transaction' means the process starting once the initiation of a payment transaction is completed and			

PUBLIC

ending once the funds placed, withdrawn, or transferred are available to the payee;			
(9) 'payment system' means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing or settlement of payment transactions;			
(10) 'payment system operator' means the legal entity legally responsible for operating a payment system;			
(11) 'payer' means a natural or legal person who holds a payment account and places a payment order from that payment account, or, where there is no payment account, a person who places a payment order;	(11) 'payer' means a natural or legal person who holds a payment account and places <u>or allows</u> a payment order from that payment account, or, where there is no payment account, a <u>natural or legal</u> person who places a payment order.		
(12) 'payee' means a natural or legal person who is the intended recipient of funds which are the subject of a payment transaction;			
(13) 'payment service user' means a natural or legal person making use of a payment service or of an electronic money service in the capacity of payer, payee, or both;			
(14) 'payment service provider' means a body as referred to in Article 2(1) or a natural			

PUBLIC

or legal person benefiting from an exemption pursuant to Articles 34, 36 and 38 of Directive (EU) [PSD3];			
(15) 'payment account' means an account held by a payment service provider in the name of one or more payment service users which is used for the execution of one or more payment transactions and allows for sending and receiving funds to and from third parties;	(15) 'payment account' means an account held by a payment service provider in the name of one or more payment service users which ~~is~~ can be used for the execution of one or more payment transactions and allows for sending and receiving funds to and from third parties	(15) 'payment account' means an account held by a payment service provider in the name of one or more payment service users which is ~~can be~~ used for the execution of one or more payment transactions and allows for sending and receiving funds to and from third parties; *[**PRES comment**: Based on the MSs' comments.]*	
(16) 'payment order' means an instruction by a payer or payee to its payment service provider requesting the execution of a payment transaction;			
(17) 'mandate' means the expression of authorisation given by the payer to the payee and (directly or indirectly via the payee) to the payer's payment service provider allowing the payee to initiate a payment transaction for debiting the payer's specified			

PUBLIC

payment account and to allow the payer's payment service provider to comply with such instructions;			
(18) 'payment instrument' means an individualised device or devices and/or set of procedures agreed between the payment service user and the payment service provider which enables the initiation of a payment transaction;			
(19) 'account servicing payment service provider' means a payment service provider providing and maintaining a payment account for a payer;	(19) 'account servicing payment service provider' means a payment service provider providing and maintaining a payment account for a ~~payer~~ payment service user.		
(20) 'payment initiation service' means a service to place a payment order at the request of the payer or of the payee with respect to a payment account held at another payment service provider;	(20) 'payment initiation service' means a service to place a payment order at the request of the payer and, as the case may be, ~~or of~~ the payee, with respect to a payment account held at another payment service provider		
(21) 'account information service' means an online service of collecting, either directly or through a technical service provider, and consolidating information held on one or more payment accounts of a payment service	(21) 'account information service' means an online service where a provider accesses one or several payment accounts held by the payment service user with one or		

PUBLIC

user with one or several account servicing payment service providers;	several account servicing payment service providers that is available online in order to access the data available therein with a view to providing a service of aggregation and/or consolidation of data to the payment service user or, subject to the consent of the payment service user issued in accordance with Regulation (EU) 2016/679, to transmitting the data to another entity that will provide said service to the payment service user. ~~of collecting, either directly or through a technical service provider, and consolidating information held on one or more payment accounts of a payment service user with one or several account servicing payment service providers.~~		
(22) 'payment initiation service provider' means a payment service provider providing payment initiation services;			
(23) 'account information service provider' means a payment service provider providing account information services;	(23) 'account information service provider' ~~means a payment service provider providing account~~		

PUBLIC

	~~information services;~~ means an account information service provider as defined in Article 2 point (20) of Directive XXX [PSD3];		
(24) 'consumer' means a natural person who, in payment service contracts covered by this Regulation, is acting for purposes other than his or her trade, business or profession;			
(25) 'framework contract' means a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account;			
(26) 'money remittance' means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, or where such funds are received on behalf of and made available to the payee;			
(27) 'direct debit' means a payment service for debiting a payer's payment account,			

PUBLIC

where a payment transaction is initiated by the payee on the basis of a mandate given by the payer to the payee, to the payee's payment service provider or to the payer's own payment service provider;			
(28) 'credit transfer' means a payment service, including instant credit transfers, 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 payment service provider which holds the payer's payment account, based on an instruction given by the payer;			
(29) 'instant credit transfer' means a credit transfer which is immediately executed, regardless of the day or hour;		(29) 'instant credit transfer' means a credit transfer which is executed immediately ~~executed~~, 24 hours a day and on any calendar day ~~regardless of the day or hour~~; *[**PRES comment:** Alignment with the definition introduced by IPR (Regulation EU 2024/886) as suggested by one Member State.]*	

(30) 'funds' means central bank money issued for retail use, scriptural money and electronic money;		(30) 'funds' means central bank money issued for retail use, scriptural money and electronic money, including electronic money tokens; ***[PRES comment:*** *The proposal presented at the February CWP meeting.]*	
(31) 'value date' means a reference time used by a payment service provider for the calculation of interest on the funds debited from or credited to a payment account;			
(32) 'reference exchange rate' means the exchange rate which is used as the basis to calculate any currency conversion cost and which is disclosed by the payment service provider or comes from a publicly available source;			
(33) 'reference interest rate' means the interest rate which is used as the basis for calculating any interest to be applied and which comes from a publicly available source which can be verified by both parties to a payment service contract;			
(34) 'authentication' means a procedure which allows the payment service provider to			

PUBLIC

verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials;			
(35) 'strong customer authentication' means an authentication which is based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;			
(36) 'technical service provider' means a provider of services which support the provision of payment services, without entering at any time into possession of the funds to be transferred;			
(37) 'personalised security credentials' means personalised features provided by the payment service provider to a payment service user for the purposes of authentication;	(37) 'personalised security credentials' means personalised features provided by the payment service provider to a payment service user for the purposes of		

PUBLIC

	authentication, and taking into account Article 36(6) ~~of PSR~~;		
(38) 'sensitive payment data' means data which can be used to carry out fraud, including personalised security credentials;	(38) 'sensitive payment data' means data which can be used to carry out fraud, including personalised security credentials, and taking into account Article 44(2);		
(39) 'unique identifier' means a combination of letters, numbers or symbols specified by the payment service provider to the payment service user and to be provided by the payment service user to identify unambiguously another payment service user or the payment account of that other payment service user for a payment transaction;			
(40) 'means of distance communication' means a method which, without the simultaneous physical presence of the payment service provider and the payment service user, may be used for the conclusion of a payment services contract;			
(41) 'durable medium' means any instrument which enables the payment service user to store information addressed personally to that payment service user in a way accessible for future reference for a period of time			

PUBLIC

adequate to the purposes of the information and which allows the unchanged reproduction of the information stored;			
(42) 'microenterprise' means an enterprise which at the time of conclusion of the payment service contract is an enterprise as defined in Article 1 and Article 2(1) and (3) of the Annex to Recommendation 2003/361/EC;			
(43) 'business day' means a day on which the payment service provider of the payer or of the payee involved in the execution of a payment transaction is open for business to execute a payment transaction;			
(44) 'agent' means a natural or legal person who acts on behalf of a payment institution in providing payment services, with the exclusion of electronic money services;	(44) 'agent' ~~means a natural or legal person who acts on behalf of a payment institution in providing payment services, with the exclusion of electronic money services;~~ means an agent as defined in Article 2 point (28) of Directive XXX [PSD3];		
(45) 'branch' means a place of business other than the head office which is a part of a payment institution, which has no legal personality and which carries out directly some or all of the transactions inherent in the	(45) 'branch' ~~means a place of business other than the head office which is a part of a payment institution, which has no legal personality and which carries out~~		

PUBLIC

business of a payment institution; all of the places of business set up in the same Member State by a payment institution with a head office in another Member State shall be regarded as a single branch;	~~directly some or all of the transactions inherent in the business of a payment institution; all of the places of business set up in the same Member State by a payment institution with a head office in another Member State shall be regarded as a single branch;~~ means a branch as defined in Article 2 point (29) of Directive XXX [PSD3];		
(46) 'group' means a group of undertakings that are linked to each other by a relationship as referred to in Article 22(1), points (2) or (7) of Directive 2013/34/EU of the European Parliament and of the Council[36] or undertakings as referred to in Articles 4, 5, 6 and 7 of Commission Delegated Regulation (EU) No 241/2014[37], which are linked to each other by a relationship as referred to in Article 10(1) or Article 113(6), first subparagraph, or 113(7), first subparagraph of Regulation (EU) No 575/2013;	(46) 'group' ~~means a group of undertakings that are linked to each other by a relationship as referred to in Article 22(1), points (2) or (7) of Directive 2013/34/EU of the European Parliament and of the Council or undertakings as referred to in Articles 4, 5, 6 and 7 of Commission Delegated Regulation (EU) No 241/2014, which are linked to each other by a relationship as referred to in~~		

[36] Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC (OJ L 182, 29.6.2013, p. 19).

[37] Commission Delegated Regulation (EU) No 241/2014 of 7 January 2014 supplementing Regulation (EU) No 575/2013 of the European Parliament and of the Council with regard to regulatory technical standards for Own Funds requirements for institutions (OJ L 74, 14.3.2014, p. 8).

PUBLIC

	~~Article 10(1) or Article 113(6), first subparagraph, or 113(7), first subparagraph of Regulation (EU) No 575/2013;~~ means a group as defined in Article 2 point (30) of Directive XXX [PSD3];		
(47) 'digital content' means goods or services which are produced and supplied in digital form, the use or consumption of which is restricted to a technical device and which do not include in any way the use or consumption of physical goods or services;			
(48) 'acquiring of payment transactions' means a payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee;			
(49) 'issuing of payment instruments' means a payment service by a payment service provider contracting to provide a payer with a payment instrument to initiate and process the payer's payment transactions;			
(50) 'electronic money' means electronically, including magnetically, stored monetary value as represented by a claim on			

PUBLIC

the issuer which is issued on the receipt of funds for the purpose of making payment transactions and which is accepted by other natural or legal persons than the issuer;			
(51) 'distributor' means a natural or legal person that distributes or redeems electronic money on behalf of a payment institution;	~~(51) 'distributor' means a natural or legal person that distributes or redeems electronic money on behalf of a payment institution;~~		
(52) 'electronic money services' means the issuance of electronic money, the maintenance of payment accounts storing electronic money units, and the transfer of electronic money units;	(51 ~~52~~) 'electronic money services' means the issuance of electronic money, the maintenance of payment accounts storing electronic money units, and the transfer of electronic money units;		
(53) 'commercial trade name' means the name which is commonly used by the payee to identify itself to the payer;	(52 ~~53~~) 'commercial trade name' means the name which is commonly used by the payee to identify itself to the payer;		
(54) 'ATM deployer' means operators of automated teller machines who do not service payment accounts.	(53 ~~54~~) 'independent ATM deployer' means an ~~natural or legal person providing cash withdrawal services as referred to Annex I, point 1, and who is not account servicing payment service provider, according to Article 3 (19) of PSR and does not provide other payment services referred to in~~	(53 ~~54~~) 'independent ~~-~~ATM deployer' means an ~~natural or legal person providing cash withdrawal services as referred to Annex I, point 1, and who is not account servicing payment service provider, according to~~	

	~~the Annex I.~~ independent ATM deployer as defined in Article 2 point (35) of Directive XXX [PSD3]. ~~(54) 'ATM deployer' means operators of automated teller machines who do not service payment accounts;~~	~~Article 3 (19) of PSR and does not provide other payment services referred to in the Annex I.~~ ~~independent~~ ATM deployer as defined in Article 2 point (35) of Directive XXX [PSD3]. ~~(54) 'ATM deployer' means operators of automated teller machines who do not service payment accounts;~~	
(55) 'payment institution providing electronic money services' means a payment institution which provides the services of issuance of electronic money, maintenance of payment accounts storing electronic money units, and transfer of electronic money units, whether or not it also provides any of the services referred to in Annex I.	(54 ~~55~~) 'payment institution providing electronic money services~~'~~ ~~means a payment institution which provides the services of issuance of electronic money, maintenance of payment accounts storing electronic money units, and transfer of electronic money units, whether or not it also provides any of the services referred to in Annex I~~ means a payment institution providing electronic money services as defined in Article 2 point (35) of Directive XXX [PSD3]; 	(54 ~~55~~) 'payment institution providing electronic money services~~'~~ ~~means a payment institution which provides the services of issuance of electronic money, maintenance of payment accounts storing electronic money units, and transfer of electronic money units, whether or not it also provides any of the services referred to in Annex I~~ means a payment institution providing electronic money	

PUBLIC

		services as defined in Article 2 point (365) of Directive XXX [PSD3];	
	(55 ~~56~~) "merchant-initiated transaction (MIT)" means a payment transaction where the payer has given a mandate authorizing the payee to place a payment order for a payment transaction or a series of payment transactions through a particular payment instrument that is issued to be used by the payer to place payment orders for the payment transactions, and where the mandate is based on an agreement between the payer and the payee for the provision of products or services, provided that those transactions do not need to be preceded by a specific action of the payer to trigger their initiation by the payee.		
	(56 ~~57~~) "mail order or telephone order transaction (MOTO)" means a payment transaction for which payment orders are placed by the payer with modalities other than the		

PUBLIC

	use of electronic platforms or devices, such as paper-based payment orders, mail orders or telephone orders, irrespective of whether or not the execution of the transaction is performed electronically.		
	(57) 'electronic communications service provider' means any provider which provides the services falling under the scope of Directive (EU) 2018/1972 (European electronic communications code).		
		(58) 'aggregated live mid-market benchmark rate' means a rate that represents the mid-point between the buy and sell prices of a currency pair in the foreign exchange market, and that is calculated by combining data from multiple sources to provide an accurate and real-time reflection of the market conditions;	

PUBLIC

		(59) 'periodic penalty payments' means periodic pecuniary enforcement measures, aimed at ending ongoing breaches of this Regulation or breaches of any decisions issued by a competent authority on the basis of those provisions and compelling the natural or legal person to return to compliance with the infringed provisions or decisions; ***[PRES comment:*** *The definition inserted on the basis of the Member States's comment that for the sake of consistency and legal certainty, such a definition should be introduced in alignment with the solution adopted in the CRD VI.]*	
		(60) 'electronic money token' means an electronic money token as defined in	

		Article 3(1)(7) of Regulation (EU) 2023/1114; ***[PRES comment:*** *The proposal presented at the February CWP meeting.]*	
		(61) 'crypto-asset service provider' means a crypto-asset service provider as defined in Article 3(1)(15) of Regulation (EU) 2023/1114; ***[PRES comment:*** *The proposal presented at the February CWP meeting.]*	
		(62) 'self-hosted address' means a self-hosted address as defined in Article 3 (20) of Regulation (EU) 2023/1113; ***[PRES comment:*** *The proposal presented at the February CWP meeting.]*	
		(63) 'custodial wallet' means a crypto-asset wallet address where a crypto-asset service provider ensures the safekeeping or controlling, on behalf of its client, of	

		crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys. ***[PRES comment:*** *The proposal presented at the February CWP meeting.]*	
TITLE II			
TRANSPARENCY OF CONDITIONS AND INFORMATION REQUIREMENTS FOR PAYMENT SERVICES			
CHAPTER 1			
General rules			
Article 4			
Scope			
1. This Title applies to single payment transactions, framework contracts and payment transactions covered by those contracts. The parties to such single payment transactions, framework contracts and payment transactions covered by them may agree that this Title shall not apply in whole or in part where the payment service user is not a consumer.			

PUBLIC

2. Member States may apply this Title to microenterprises in the same way as to consumers.			
3. Member States shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 2, by the date of application of this Regulation and, without delay, any subsequent amendment affecting them.			
Article 5			
Currency and currency conversion			
1. Payments shall be made in the currency agreed between the parties.		1. Payment~~s~~ transactions shall be made in the currency agreed between the parties. ***[PRES comment:*** *Amendment follows comment of one Member State.]*	
2. Where a currency conversion service is offered prior to the initiation of the payment transaction and where that currency conversion service is offered at an ATM, at the point of sale or by the payee, the party offering the currency conversion service to			

PUBLIC

the payer shall disclose to the payer all charges and the exchange rate to be used for converting the payment transaction.			
3. The payer shall be given the possibility to agree to the currency conversion service on that basis.			
		4. For the purposes of Articles 13(1)(f) and 20(c)(v) of this Regulation, the aggregated live mid-market benchmark rate used shall accurately reflect the market, with a maximum delay of 10 minutes or, for currencies where this is not possible, reflect the last traded price from a reputable trading venue. It shall be provided by a trusted administrator who complies with the IOSCO Principles for Financial Benchmarks.	
Article 6			
Information on additional charges or reductions			

PUBLIC

1. Where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction.	1. Where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction, in a clear, transparent and accessible format.	1. Where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction, in a clear, neutral and comprehensible manner ~~in a clear, transparent and accessible format~~. ***[PRES comment**: Amendment based on the comment of one of the Member States suggesting to introduce a uniform wording as regards the information duties in PSR.]*	
2. Where, for the use of a given payment instrument, the payment service provider or another party involved in the transaction requests a charge, it shall inform the payment service user thereof prior to the initiation of the payment transaction.	2. Where, for the use of a given payment instrument, the payment service provider or another party involved in the transaction requests a charge, it shall inform the payment service user thereof in a clear, transparent and accessible format,	2. Where, for the use of a given payment instrument, the payment service provider or another party involved in the transaction requests a charge, it shall inform the payment service user thereof in a clear, neutral and	

	prior to the initiation of the payment transaction.	comprehensible manner ~~transparent and accessible format~~, prior to the initiation of the payment transaction. ***[PRES comment**: Amendment based on the comment of one of the Member States suggesting to introduce a uniform wording as regards the information duties in PSR.]*	
3. The payer shall only be obliged to pay for the charges referred to in paragraphs 1 and 2 if their full amount was made known prior to the initiation of the payment transaction.			
Article 7			
Information requirements applicable to cash withdrawal services			
Natural or legal persons providing cash withdrawal services as referred to in Article 38 of Directive (EU) [PSD3] shall provide or make available to their customers information on any charges before the	Natural or legal persons providing cash withdrawal services as referred to in Article 38 of Directive (EU) [PSD3] shall ~~provide or make available~~ display at the ATM to their	Natural or legal persons providing cash withdrawal services as referred to in Article 38 of Directive (EU) [PSD3] shall ~~provide or~~	

customer carries out the withdrawal as well as upon receipt of the cash when the transaction is completed.	customers information on any charges before the customer carries out the withdrawal ~~as well as upon receipt of the cash when the transaction is completed~~. The information shall be displayed in a clear, neutral and comprehensible manner. The information on any charges shall also be made available to the customer upon request of the customer on a durable medium when the transaction is completed. The information shall be made available in a clear, neutral and comprehensible manner.	~~make available~~ display at the ATM to their customers information on any charges before the customer carries out the withdrawal ~~as well as upon receipt of the cash when the transaction is completed~~. The information shall be displayed in a clear, neutral and comprehensible manner. The information on any charges shall also be made available to the customer upon request of the customer on a durable medium when the transaction is completed. ~~The information shall be made available in a clear, neutral and comprehensible manner.~~ ***[PRES comment**: The duplication of 2nd sentence of this paragraph.]*	
Article 8			
Charges for information			

PUBLIC

1. Payment service providers shall not charge payment service users for providing information under this Title.			
2. Payment service providers and payment service users may agree on charges for additional or more frequent information, or transmission by means of communication other than those specified in the framework contract, provided at the payment service user's request.			
3. Charges for information referred to in paragraph 2 shall be reasonable and in line with the payment service provider's actual costs.			
Article 9			
Burden of proof on information requirements			
The burden of proof shall lie with the payment service providers to prove that they have complied with the information requirements set out in this Title.			
Article 10			

PUBLIC

Derogation from information requirements for low-value payment instruments and electronic money			
In cases of payment instruments which, according to the relevant framework contract, concern only individual payment transactions that do not exceed EUR 50 or that either have a spending limit of EUR 200 or store funds that do not exceed EUR 200 at any time:	1. In cases of payment instruments which, according to the relevant framework contract, concern only individual payment transactions that do not exceed EUR 50 or that either have a spending limit of EUR 200 or store funds that do not exceed EUR 200 at any time:		
(a) by way of derogation from Articles 19, 20 and 24, the payment service provider shall provide the payer only with information on the main characteristics of the payment service, including the way in which the payment instrument can be used, liability, charges levied and other material information needed for the payer to take an informed decision as well as an indication of where any other information and conditions specified in Article 20 are made available in an easily accessible manner;			
(b) it may be agreed by the parties to the framework contract that, by way of			

PUBLIC

derogation from Article 22, the payment service provider is not required to propose changes to the conditions of the framework contract in the same way as provided for in Article 19(1);			
(c) it may be agreed by the parties to the framework contract that, by way of derogation from Articles 25 and 26, after the execution of a payment transaction:			
(i) the payment service provider provides or makes available only a reference enabling the payment service user to identify the payment transaction, the amount of the payment transaction, any charges or, in the case of several payment transactions of the same kind made to the same payee, information on the total amount and charges for those payment transactions;			
(ii) the payment service provider is not required to provide or make available information referred to in point (i) if the payment instrument is used anonymously or if the payment service provider is not otherwise technically in a position to provide it. The payment service provider shall			

PUBLIC

provide the payer with a possibility to verify the amount of funds stored.			
	2. For national payment transactions, Member States or their competent authorities may double the amounts referred to in paragraph 1. For prepaid payment instruments, Member States may increase those amounts up to EUR 500.		
		3. Member States shall by [OP please insert the date = data of application of this Regulation] notify to the Commission the provisions of their law adopted pursuant to paragraph 2. They shall, without delay, notify any subsequent amendment to such provisions. *[**PRES comment**: As it is in Article 25(4) and 26(4), the PRES suggests adding the garagraph on the notification to the Commission on adopted national measures.*	

PUBLIC

		The same approach is applied in PSD2.]	
CHAPTER 2			
Single payment transactions			
Article 11			
Scope			
1. This Chapter applies to single payment transactions not covered by a framework contract.			
2. Where a payment order for a single payment transaction is transmitted by a payment instrument covered by a framework contract, the payment service provider shall not be obliged to provide or make available information which is already given to the payment service user on the basis of a framework contract with another payment service provider or which will be given to the payment service user according to that framework contract.			
Article 12			
Prior general information			

PUBLIC

1. Before the payment service user is bound by a single payment service contract or offer, the payment service provider shall make available to the payment service user, in an easily accessible manner, the information and conditions set out in Article 13 with regard to its own services. At the payment service user's request, the payment service provider shall provide the information and conditions on paper or on another durable medium. The information and conditions shall be given in easily understandable words and in a clear and comprehensible form, in an official language of the Member State where the payment service is offered or in any other language agreed between the parties.		1. Before the payment service user is bound by a single payment service contract or offer, the payment service provider shall make available to the payment service user, in an easily accessible manner, the information and conditions set out in Article 13 with regard to its own services. At the payment service user's request, the payment service provider shall provide the information and conditions on paper or on another durable medium. The information and conditions shall be given in easily understandable words and in a clear, neutral and comprehensible manner ~~form~~, in an official language of the Member State where the payment service is offered or in any other	

		language agreed between the parties. ***[PRES comment**: Amendment based on the comment of one of the Member States suggesting to introduce a uniform wording as regards the information duties in PSR.]*	
2. If the single payment service contract has been concluded at the request of the payment service user using a means of distance communication which does not enable the payment service provider to comply with paragraph 1, the payment service provider shall fulfil its obligations under that paragraph immediately after the execution of the payment transaction.			
3. Payment service providers may also comply with their obligations under paragraph 1 by providing to payment service users a copy of the draft single payment service contract or the draft payment order including the information and conditions set out in Article 13.			

PUBLIC

Article 13			
Information and conditions			
1. Payment service providers shall provide or make available to payment service users the following information and conditions:			
(a) a specification of the information or unique identifier to be provided by the payment service user in order for a payment order to be properly placed or executed;			
(b) the maximum execution time for the payment service to be provided;			
(c) the estimated time for the funds of credit transfers and money remittance transactions to be received by the payment service provider of the payee located outside the Union;		(c) where applicable, the estimated time for the funds of credit transfers and money remittance transactions to be received by the payment service provider of the payee located outside the Union; ***[PRES comment**: Amendment based on the comment of one of the Member States suggesting addition of "where applicable", as not all*	

PUBLIC

		payment orders involve third countries.]	
(d) all charges payable by the payment service user to the payment service provider and, where applicable, a breakdown of those charges;			
(e) where applicable, the actual or reference exchange rate to be applied to the payment transaction;			
(f) where applicable, the estimated charges for currency conversion in relation to credit transfers and money remittance transactions, expressed as a percentage mark-up over the latest available applicable foreign exchange reference rate issued by the relevant central bank;	(f) where applicable, the estimated charges for currency conversion in relation to credit transfers and money remittance transactions, expressed as a monetary amount in the currency of the payer's account and as a percentage mark-up over the latest available applicable foreign exchange reference rates issued by the ~~relevant~~ ~~central bank~~ ECB or, where not available for non-euro currencies, the latest available applicable foreign exchange reference rate issued by the relevant central bank;	(f) where applicable, the estimated charges for currency conversion in relation to credit transfers and money remittance transactions, expressed as a monetary amount in the currency of the payer's account and as a percentage mark-up over an aggregated live mid-market benchmark rate as referred to in Article 5(4) ~~the latest available applicable foreign exchange reference rates issued by the relevant central bank ECB or, where not available for non-~~	

		~~euro currencies, the latest available applicable foreign exchange reference rate issued by the relevant central bank~~;	
(g) the alternative dispute resolution procedures available to the payment service user in accordance with Articles 90, 94 and 95.			
2. In addition, payment initiation service providers shall, prior to initiation, provide the payer with, or make available to the payer clear and comprehensive information on all of the following:			
(a) the name of the payment initiation service provider, the geographical address of its head office and, where applicable, the geographical address of its agent or branch established in the Member State where the payment service is offered, and any other contact details, including electronic mail address, relevant for communication with the payment initiation service provider; and			
(b) the contact details of the competent authority designated under this Regulation.			

PUBLIC

3. Where applicable, any other relevant information and conditions set out in Article 20 shall be made available to the payment service user in an easily accessible manner.			
Article 14			
Information for the payer and payee after the placement of a payment order			
Where a payment order is placed through a payment initiation service provider, the payment initiation service provider shall, immediately after initiation, provide or make available to the payer and, where applicable, to the payee all of the following data:			
(a) confirmation of the successful placement of the payment order with the payer's account servicing payment service provider;			
(b) a reference enabling the payer and the payee to identify the payment transaction and, where appropriate, the payee to identify the payer, and any information transferred with the payment transaction;			

PUBLIC

(c) the amount of the payment transaction;			
(d) where applicable, the amount of any charges payable to the payment initiation service provider for the transaction, and where applicable a breakdown of the amounts of such charges.			
Article 15			
Information for the payer's account servicing payment service provider where a payment order is placed through a payment initiation service			
Where a payment order is placed through a payment initiation service provider, the payment initiation service provider shall make available to the payer's account servicing payment service provider the reference of the payment transaction.			
Article 16			
Information for the payer after receipt of the payment order			

PUBLIC

Immediately after receipt of the payment order, the payer's payment service provider shall provide the payer with or make available to the payer, in the same way as provided for in Article 12(1), all of the following data with regard to its own services:	1. Immediately after receipt of the payment order, the payer's payment service provider shall provide the payer with or make available to the payer, in the same way as provided for in Article 12(1), all of the following data with regard to its own services:		
(a) a reference enabling the payer to identify the payment transaction and the information needed for the payer to unambiguously identify the payee, including the payee's commercial trade name;	(a) a reference enabling the payer to identify the payment transaction and the information needed for the payer to unambiguously identify the payee, including, where possible, the payee's legal and, if different therefrom, the payee's commercial trade name;		
(b) the amount of the payment transaction in the currency used in the payment order;			
(c) the amount of any charges for the payment transaction payable by the payer and, where applicable, a breakdown of the amounts of such charges;			
(d) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider or a			

PUBLIC

reference thereto, where different from the rate provided in accordance with Article 13(1), point (e), and the amount of the payment transaction after that currency conversion;			
(e) the date of receipt of the payment order.			
	2. The EBA shall develop draft regulatory technical standards to specify the identification of the payee referred to in paragraph 1, point (a), in particular regarding the dissociation of the legal person and the commercial trade name in accordance with Regulation (EU) 2024/886 Article 1(2). The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with		

PUBLIC

	Articles 10 to 14 of Regulation (EU) No 1093/2010.		
Article 17			
Information for the payee after execution			
Immediately after the execution of the payment transaction, the payee's payment service provider shall provide the payee with, or make available to the payee, in the same way as provided for in Article 12(1), all of the following data with regard to its own services:			
(a) a reference enabling the payee to identify the payment transaction and, where appropriate, the payer and any information transferred with the payment transaction;			
(b) the amount of the payment transaction in the currency in which the funds are at the payee's disposal;			
(c) the amount of any charges for the payment transaction payable by the payee and, where applicable, a breakdown of the amounts of such charges;			
(d) where applicable, the exchange rate used in the payment transaction by the			

PUBLIC

payee's payment service provider, and the amount of the payment transaction before that currency conversion;			
(e) the credit value date.			
CHAPTER 3			
Framework contracts			
Article 18			
Scope			
This Chapter applies to payment transactions covered by a framework contract.			
Article 19			
Prior general information			
1. In good time before the payment service user is bound by any framework contract or offer, the payment service provider shall provide the payment service user on paper or on another durable medium with the information and conditions set out in Article 20. The information and conditions shall be given in easily understandable words and in a clear and comprehensible form, in an official language of the Member State where		1. In good time before the payment service user is bound by any framework contract or offer, the payment service provider shall provide the payment service user on paper or on another durable medium with the information and conditions set out in Article 20. The	

the payment service is offered or in any other language agreed between the parties.		information and conditions shall be given in easily understandable words and in a clear, neutral and comprehensible manner ~~form~~, in an official language of the Member State where the payment service is offered or in any other language agreed between the parties. ***[PRES comment**: Amendment based on the comment of one of the Member States suggesting to introduce a uniform wording as regards the information duties in PSR.]*	
2. Where the framework contract has been concluded at the request of the payment service user using a means of distance communication which does not enable the payment service provider to comply with paragraph 1, the payment service provider shall fulfil its obligations under that			

PUBLIC

paragraph immediately after conclusion of the framework contract.			
3. Payment service providers may also comply with their obligations under paragraph 1 by providing to payment service users a copy of the draft framework contract including the information and conditions set out in Article 20.			
Article 20			
Information and conditions			
The payment service provider shall provide the following information and conditions to the payment service user:			
(a) on the payment service provider:			
(i) the name of the payment service provider, the geographical address of its head office and, where applicable, the geographical address of its agent, distributor or branch established in the Member State where the payment service is offered, and any other address, including electronic mail address, relevant for communication with the payment service provider;		(i) the name of the payment service provider, the geographical address of its head office and, where applicable, the geographical address of its agent~~,~~ ~~distributor~~ or branch established in the Member State where the payment service is offered, and any	

PUBLIC

		other address, including electronic mail address, relevant for communication with the payment service provider;	
(ii) the particulars of the relevant supervisory authorities designated under Directive (EU) [PSD3] and of the register provided for in Articles 17 and 18 of that Directive or of any other relevant public register of authorisation of the payment service provider and the registration number or equivalent means of identification in that register;			
(b) on the use of the payment service:			
(i) a description of the main characteristics of the payment service to be provided;			
(ii) a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly placed or executed;			
(iii) the form of and procedure for placing a payment order or giving permission to execute a payment transaction and			

PUBLIC

withdrawal of such permission in accordance with Articles 49 and 66;			
(iv) a reference to the time of receipt of a payment order in accordance with Article 64 and the cut-off time, if any, established by the payment service provider;			
(v) the maximum execution time for the payment services to be provided;			
(vi) the estimated time for the funds of credit transfers to be received by the payment service provider of the payee located outside the Union;		(vi) where applicable, the estimated time for the funds of credit transfers to be received by the payment service provider of the payee located outside the Union; ***[PRES comment**: Amendment based on the comment of one of the Member States suggesting addition of "where applicable", as not all payment orders involve third countries.]*	
(vii) whether there is a possibility to agree on spending limits for the use of the payment instrument in accordance with Article 51(1);			

PUBLIC

(viii) in the case of co-badged card-based payment instruments, the payment service user's rights under Article 8 of Regulation (EU) 2015/751;			
(c) on charges, interest and exchange rates:			
(i) all charges payable by the payment service user to the payment service provider including those connected to the manner in and frequency with which information under this Regulation is provided or made available and, where applicable, the breakdown of the amounts of such charges;			
(ii) all charges, if any, for domestic, automated teller machines (ATMs) withdrawals payable by payment service users to their payment service provider at an ATM of:			
(1) their payment service provider;			
(2) a payment service provider belonging to the same network of ATMs as the user's payment service provider;			
(3) a payment service provider belonging to a network of ATMs with whom the user's payment service provider has a contractual relationship;			

PUBLIC

(4) an ATM provider not servicing payment accounts when offering cash withdrawal services;			
(iii) where applicable, the interest and exchange rates to be applied or, if reference interest and exchange rates are to be used, the method of calculating the actual interest, and the relevant date and index or base for determining such reference interest or exchange rate;			
(iv) where agreed, the immediate application of changes in reference interest or exchange rate and information requirements relating to the changes in accordance with Article 22(3);			
(v) where applicable, the estimated charges for currency conversion services in relation to a credit transfer expressed as a percentage mark-up over the latest available applicable foreign exchange reference rate issued by the relevant central bank;	(v) where applicable, the estimated charges for currency conversion services in relation to a credit transfer expressed as a monetary amount in the currency of the payer's account and as a percentage mark-up over the latest available applicable foreign exchange reference rates issued by the ~~relevant central bank~~ ECB or where not available for non-euro currencies, the latest available	(v) where applicable, the estimated charges for currency conversion services in relation to a credit transfer expressed as a monetary amount in the currency of the payer's account and as a percentage mark-up over an aggregated live mid-market benchmark rate as referred to in Article 5(4) ~~the latest~~	

	applicable foreign exchange reference rate issued by the relevant central bank;	~~available applicable foreign exchange reference rates issued by the relevant central bank ECB or where not available for non-euro currencies, the latest available applicable foreign exchange reference rate issued by the relevant central bank~~;	
(d) on communication:			
(i) where applicable, the means of communication, including the technical requirements for the payment service user's equipment and software, agreed between the parties for the transmission of information or notifications under this Regulation;			
(ii) the manner in, and frequency with which, information under this Regulation is to be provided or made available;			
(iii) the language or languages in which the framework contract will be concluded and communication during that contractual relationship undertaken;			
(iv) the payment service user's right to receive the contractual terms of the			

PUBLIC

framework contract and information and conditions in accordance with Article 21;			
(e) on safeguards and corrective measures:			
(i) where applicable, a description of the steps that the payment service user is to take in order to keep safe a payment instrument and how to notify the payment service provider for the purposes of Article 52, point (b);			
(ii) the secure procedure for notification of the payment service user by the payment service provider in the event of suspected or actual fraud or security threats;			
(iii) where agreed, the conditions under which the payment service provider reserves the right to block a payment instrument in accordance with Article 51;			
(iv) the liability of the payer in accordance with Article 57(5), Article 59(3) and Article 60, including information on the relevant amount;			
(v) how and within what period of time the payment service user is to notify the payment service provider, and the police in case of impersonation fraud referred to in			

PUBLIC

Article 59, of any unauthorised or incorrectly initiated or executed payment transaction or of any authorised credit transfer made following an incorrect application of the name and unique identifier matching verification service or impersonation fraud, in accordance with Article 54;			
(vi) the payment service provider's liability for unauthorised payment transactions in accordance with Article 56, for the incorrect application of the name and unique identifier matching verification service in accordance with Article 57, and for impersonation fraud in accordance with Article 59;			
(vii) the liability of the payment service provider for the initiation or execution of payment transactions in accordance with Articles 75 and 76;			
(viii) the conditions for refund in accordance with Articles 62 and 63;			
(f) on changes to, and termination of, the framework contract:			
(i) where agreed, information that the payment service user will be deemed to have accepted changes in the conditions in			

PUBLIC

accordance with Article 22, unless the payment service user notifies the payment service provider before the date of their proposed date of entry into force that they are not accepted;			
(ii) the duration of the framework contract;			
(iii) the right of the payment service user to terminate the framework contract and any agreements relating to termination in accordance with Article 22(1) and Article 23;			
(g) on redress:			
(i) any contractual clause on the law applicable to the framework contract or the competent courts;			
(ii) the alternative dispute resolution procedures available to the payment service user in accordance with Articles 90, 94 and 95.			
Article 21			
Accessibility of information and conditions of the framework contract			

PUBLIC

At any time during the contractual relationship the payment service user shall have a right to receive, on request, the contractual terms of the framework contract and the information and conditions set out in Article 20 on paper or on another durable medium.			
Article 22			
Changes in conditions of the framework contract			
1. The payment service provider shall propose any changes in the framework contract or in the information and conditions set out in Article 20 in the same way as provided for in Article 19(1) and no later than 2 months before their proposed date of application. The payment service user can either accept or reject the changes before the date of their proposed date of entry into force.			
2. Where applicable, in accordance with Article 20, point (f)(i), the payment service provider shall inform the payment service user that the payment service user is to be deemed to have accepted those changes if the			

PUBLIC

payment service user does not notify the payment service provider before the proposed date of their entry into force that they are not accepted. The payment service provider shall also inform the payment service user that, if the payment service user rejects those changes, the payment service user has the right to terminate the framework contract free of charge and with effect at any time until the date when the changes would have applied.			
3. Changes in the interest or exchange rates may be applied by the payment service provider immediately and without notice, provided that such a right is agreed upon in the framework contract and that the changes in the interest or exchange rates are based on the reference interest or exchange rates agreed on in accordance with Article 20, point (c)(iii) and (iv). The payment service provider shall inform the payment service user of any change in the interest rate at the earliest opportunity in the same way as provided for in Article 19(1), unless the parties have agreed on a specific frequency or manner in which the information is to be			

PUBLIC

provided or made available. However, changes in interest or exchange rates which are more favourable to the payment service users, may be applied by the payment service provider without notice.			
4. The payment service provider shall implement and calculate changes in the interest or exchange rate used in payment transactions in a neutral manner that does not discriminate against payment service users.			
	5. Member States may ~~provide for more favourable provisions for the payment service user on changes to the conditions of the framework contract made by the payment service provider~~maintain or introduce restrictions or prohibitions on unilateral changes in the conditions of a framework contract.		
	6. Member States shall by [OP please insert the date = data of application of this Regulation] notify to the Commission the provisions of their law adopted pursuant to paragraph 5. They shall, without undue delay,		

PUBLIC

	notify any subsequent amendment to such provisions.		
Article 23			
Termination			
1. The payment service user may terminate the framework contract at any time, unless the parties have agreed on a period of notice. Such a period shall not exceed 1 month.			
2. Termination of the framework contract shall be free of charge for the payment service user except where the contract has been in force for less than 6 months. Charges, if any, for termination of the framework contract shall be appropriate and in line with costs. Where, under the framework contract, payment services are offered jointly with technical services aimed at supporting the provision of payment services and provided by the payment service provider or by a third party the payment service provider has partnered with, such technical services shall be subject to the same			

PUBLIC

framework contract requirements on termination fees.			
3. If agreed in the framework contract, the payment service provider may terminate a framework contract concluded for an indefinite period by giving at least 2 months' notice in the same way as provided for in Article 19(1).			
4. Charges for payment services levied on a regular basis shall be payable by the payment service user only proportionally up to the termination of the contract. If such charges are paid in advance, those charges shall be reimbursed proportionally by the payment service provider.			
5. The provisions of this Article are without prejudice to the Member States' laws and regulations governing the rights of the parties to declare the framework contract unenforceable or void.			
6. Member States may provide for more favourable provisions on termination for payment service users.			
7. Member States shall by [OP please insert the date = data of application of this Regulation] notify to the Commission the			

PUBLIC

provisions of their law adopted pursuant to paragraph 6. They shall, without delay, notify any subsequent amendment to such provisions.			
Article 24			
Information before execution of individual payment transactions			
In the case of an individual payment transaction initiated by the payer under a framework contract, a payment service provider shall, at the payer's request for this specific payment transaction, provide explicit information on all of the following:			
(a) the maximum execution time;			
(b) the charges payable by the payer;			
(c) where applicable, a breakdown of the amounts of any charges.			
Article 25			
Information for the payer on individual payment transactions			
1. After the amount of an individual payment transaction is debited from the			

PUBLIC

payer's account or, where the payer does not use a payment account, after receipt of the payment order, the payer's payment service provider shall provide the payer, without undue delay and in the same way as laid down in Article 19(1), with all of the following information:			
(a) a reference enabling the payer to identify each the payment transaction and the information needed to unambiguously identify the payee, including the payee's commercial trade name;	(a) a reference enabling the payer to identify each ~~the~~ payment transaction and the information needed to unambiguously identify the payee, including the payee's legal name, and, if different therefrom, the payee's commercial trade name;	(a) a reference enabling the payer to identify each ~~the~~ payment transaction and the information needed to unambiguously identify the payee, including, where possible, the payee's legal name, and, if different therefrom, the payee's commercial trade name; *[**PRES comment**: As indicated by one MS, this obligation should in principle be similar to the obligation under Article 16 PSR, so that here too only information available to the PSP must be passed on.]*	

PUBLIC

(b) the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency used for the payment order;			
(c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges, or the interest payable by the payer;			
(d) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider, and the amount of the payment transaction after that currency conversion;			
(e) the debit value date or the date of receipt of the payment order.			
2. A framework contract shall include a condition that the payer may require the information referred to in paragraph 1 to be provided or made available periodically, at least once a month, free of charge and in an agreed manner which allows the payer to store and reproduce information unchanged.			
3. Member States may require payment service providers to provide information on paper or on another durable medium at least once a month, free of charge.			

PUBLIC

4. Member States shall by [OP please insert the date = data of application of this Regulation] notify to the Commission the provisions of their law adopted pursuant to paragraph 3. They shall, without delay, notify any subsequent amendment to such provisions.			
Article 26			
Information for the payee on individual payment transactions			
1. After the execution of an individual payment transaction, the payee's payment service provider shall provide the payee without undue delay in the same way as laid down in Article 19(1) with all of the following information:			
(a) a reference enabling the payee to identify the payment transaction and the payer, and any information transferred with the payment transaction;			
(b) the amount of the payment transaction in the currency in which the payee's payment account is credited;			

PUBLIC

(c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges, or the interest payable by the payee;			
(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion;			
(e) the credit value date.			
2. A framework contract may include a condition that the information referred to in paragraph 1 is to be provided or made available periodically, at least once a month and in an agreed manner which allows the payee to store and reproduce information unchanged.			
3. Member States may require payment service providers to provide information on paper or on another durable medium at least once a month, free of charge.			
4. Member States shall by [OP please insert the date = data of application of this Regulation] notify to the Commission the provisions of their law adopted pursuant to paragraph 3. They shall, without delay, notify			

PUBLIC

any subsequent amendment to such provisions.			
TITLE III			
RIGHTS AND OBLIGATIONS IN RELATION TO THE PROVISION AND USE OF PAYMENT SERVICES			
CHAPTER 1			
Common provisions			
Article 27			
Scope			
1. Where the payment service user is not a consumer, the payment service user and the payment service provider may agree that Article 28(1), Article 49(7), and Articles 55, 60, 62, 63, 66, 75 and 76 do not apply in whole or in part. The payment service user and the payment service provider may also agree on time limits that are different from those laid down in Article 54.			
2. Member States may provide that Article 95 does not apply where the payment service user is not a consumer.			
3. Member States may provide that provisions in this Title are applied to			

PUBLIC

microenterprises in the same way as to consumers.			
4. Member States shall [OP please insert the date = data of application of this Regulation] notify to the Commission the provisions of their law adopted pursuant to paragraph 2 and 3. They shall, without delay, notify any subsequent amendment to such provisions.			
Article 28			
Charges applicable			
1. The payment service provider shall not charge the payment service user for fulfilment of its information obligations or corrective and preventive measures under this Title, unless otherwise specified in Article 65(1), Article 66(5) and Article 74(4). Those charges shall be agreed between the payment service user and the payment service provider and shall be reasonable and in line with the payment service provider's actual costs.			
2. For payment transactions provided within the Union, where both the payer's and			

PUBLIC

the payee's payment service providers are, or the sole payment service provider in the payment transaction is, located in the Union, the payee shall pay the charges levied by his payment service provider, and the payer shall pay the charges levied by his payment service provider.			
3. The payee shall not request charges for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751 and for credit transfers, including instant credit transfers, and direct debit transactions within the Union.			
4. Member States may extend the prohibition or limit the right of the payee to request charges for the use of payment instruments other than the ones referred to in paragraph 3, taking into account the need to encourage competition and promote the use of efficient payment instruments.			
5. Without prejudice to paragraphs 3 and 4 and for instruments not covered in those paragraphs, the payment service provider shall not prevent the payee from requesting from the payer a charge, offering			

PUBLIC

him a reduction or otherwise steering the payer towards the use of a given payment instrument. Any charges applied shall not exceed the direct costs borne by the payee for the use of the specific payment instrument.			
6. Member States shall [OP please insert the date = data of application of this Regulation] notify to the Commission the provisions of their law adopted pursuant to paragraph 4. They shall, without delay, notify any subsequent amendment to such provisions.			
Article 29			
Derogation for low value payment instruments and electronic money			
1. In the case of payment instruments which, according to the framework contract, solely concern individual payment transactions not exceeding EUR 50 or which either have a spending limit of EUR 200, or store funds which do not exceed EUR 200 at any time, payment service providers may agree with their payment service users that:			

PUBLIC

(a) Article 52, point (b), Article 53(1), points (c) and (d) , and Article 60(4) do not apply if the payment instrument does not allow its blocking or prevention of its further use;			
(b) Articles 55 and 56, and Article 60(1) and (4), do not apply if the payment instrument is used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised;			
(c) by way of derogation from Article 65(1), the payment service provider is not required to notify the payment service user of the refusal of a payment order, if the non-execution is apparent from the context;			
(d) by way of derogation from Article 66, the payer shall not revoke the payment order after transmitting the payment order or authorising the payment transaction to the payee;			
(e) by way of derogation from Articles 69 and 70, other execution periods apply.			
2. Articles 56 and 60 shall apply also to electronic money, except where the payer's			

PUBLIC

payment service provider does not have the ability to freeze the payment account on which the electronic money is stored or block the payment instrument. Member States may limit that derogation to payment accounts on which the electronic money is stored or to payment instruments of a certain value.			
3. Member States shall, by the date of application of this Regulation, notify to the Commission the provisions of their law adopted pursuant to paragraph 2. They shall, without delay, notify any subsequent amendment to such provisions.			
Article 30			
Issuance and redeemability of electronic money			
1. Issuers of electronic money shall issue electronic money at par value on the receipt of funds.			
2. Upon request by the holder of the electronic money, the issuer of the electronic money shall redeem, at any moment and at par value, the monetary value of the electronic money held.			

PUBLIC

3. The contract between the issuer of the electronic money and the holder of the electronic money shall clearly and prominently state the conditions of redemption, including any applicable fees, and the electronic money holder shall be informed of those conditions before being bound by any contract or offer.			
4. Redemption of electronic money may be subject to a fee only if stated in the contract in accordance with paragraph 3 and only in any of the following cases:			
(a) where the holder of electronic money requests redemption before the termination of the contract;			
(b) where the contract provides for a termination date and the holder of electronic money terminates the contract before that date;			
(c) where redemption is requested more than one year after the date of termination of the contract.			
Any such fee shall be proportionate to and commensurate with the actual costs incurred by the electronic money issuer.			

PUBLIC

5. Where the holder of electronic money requests redemption before the termination of the contract, the holder may request redemption of the electronic money in whole or in part.			
6. Where redemption is requested by the holder of the electronic money on the date of the termination of the contract, or up to one year after such termination, the issuer of the electronic money shall do either of the following:			
(a) Redeem the total monetary value of the electronic money; or			
(b) Redeem all funds requested by the electronic money holder where the payment institution carries out one or more of the activities as referred to in Article 10(1)(c) of Directive XXX [PSD3] and it is unknown in advance what proportion of funds is to be used as electronic money by electronic money holders.			
7. Notwithstanding paragraphs 4, 5 and 6, redemption rights of a person, other than a consumer, who accepts electronic money shall be subject to the contractual agreement			

PUBLIC

between the electronic money issuer and that person.			
8. A payment institution providing electronic money services shall not grant to the holder of electronic money interest or any other benefit related to the length of time during which he or she holds the electronic money.			
CHAPTER 2			
Access to payment systems and to accounts maintained with credit institutions			
Article 31			
Access to payment systems			
1. Payment system operators shall have in place objective non-discriminatory, transparent and proportionate rules on access to a payment system by authorised or registered payment service providers that are legal persons. Payment system operators shall not inhibit access to a payment system more than is necessary to safeguard against specific risks, including where applicable settlement risk, operational risk, credit risk, liquidity risk and business risk or more than			

PUBLIC

is necessary to protect the financial and operational stability of the payment system.			
2. A payment system operator shall make publicly available its rules and procedures for admission to participation to that payment system and the criteria and methodology it uses for risk assessment of applicants for participation.			
3. Upon receiving an application for participation by a payment service provider, a payment system operator shall assess the relevant risks of granting the applicant payment service provider access to the system. A payment system operator shall only refuse participation to an applicant payment service provider where the applicant poses risks to the system, as referred to in paragraph 1. The payment system operator shall notify that applicant payment service provider in writing whether the request for participation is granted or refused and shall provide full reasons for any refusal.			
4. Paragraphs 1, 2 and 3 shall not apply to payment systems composed exclusively of			

PUBLIC

payment service providers belonging to the same group.			
5. Payment system operators shall not have in place any of the following requirements:			
(a) restrictive rules on effective membership in other payment systems;			
(b) rules which discriminate between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of members;			
(c) restrictions on the basis of institutional status.			
6. A participant of a payment system that allows an authorised or registered payment service provider that is not a participant of the payment system to pass transfer orders through that payment system shall, when requested, give the same possibility to other authorised or registered payment service providers in an objective, proportionate, transparent and non-discriminatory manner. In case of a rejection of such request, the participant of a payment system shall provide any requesting payment			

PUBLIC

service provider with full reasons for such rejection.			
7. For payment systems that are not covered by Eurosystem oversight, pursuant to Regulation (EU) No 795/2014, Member States shall designate a competent authority responsible for oversight of payment systems to ensure enforcement of paragraphs 1 2, 3, 5 and 6 by payment systems governed by their national law.			
Article 32			
Provision by credit institutions of payment accounts to payment institutions			
	1. A payment institution, its agents and applicants for a license as a payment institution shall have access to credit institutions' payment accounts on an objective, non-discriminatory and proportionate basis. Such access shall be sufficiently extensive as to allow payment institutions to provide payment services in an unhindered and efficient manner.		

1. A credit institution shall only refuse to open or shall only close a payment account for a payment institution for its agents or distributors or for an applicant for a license as a payment institution in the following cases:	2. A credit institution shall only refuse to open or shall only close a payment account for a payment institution, for its agents ~~or distributors~~ or for an applicant for a license as a payment institution in the following cases:	2. A credit institution may ~~shall~~ only refuse to open or may ~~shall~~ only close a payment account for a payment institution, for its agents ~~or distributors~~ or for an applicant for a license as a payment institution in the following cases: ***[PRES comment**: Based on the comment of one of the Member States suggesting that such amendment would be in line with recital 36, according to which "credit institutions should be able to refuse the provision of a payment account when […]". In the view of this MS, it is crucial to avoid any automatism in this respect and to ensure the discretionality of the credit institution, also with a view at safeguarding the interest*	

PUBLIC

		of the payment institutions' clients.	
(a) The credit institution has serious grounds to suspect defective money laundering or terrorism financing controls by the applicant or that illegal activities are being committed either by the applicant or its customers;	(a) ~~The credit institution has serious grounds to suspect defective money laundering or terrorism financing controls by the applicant or that illegal activities are being committed either by the applicant or its customers~~ Where opening or maintaining such an account would result in an infringement of Regulation (EU) of the European Parliament and of the Council[38];		
(b) there is or has been a breach of contract committed by the applicant for an account;	(b) there is or has been a substantive breach of contract committed by the ~~applicant for an account~~ payment institution or its agents;		
(c) insufficient information and documents have been received from the applicant for an account;	(c) insufficient information ~~and~~ or documents have been received from the applicant for an account~~;~~**.**		

38 OP: Please insert in the text the number of the Regulation contained in document 2021/0239(COD) (Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - COM/2021/420 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.

PUBLIC

(d) the applicant for an account or its business model presents an excessive risk profile;	~~(d) the applicant for an account or its business model presents an excessive risk profile;~~		
(e) the applicant for an account would present a disproportionately high compliance cost for the credit institution.	~~(e) the applicant for an account would present a disproportionately high compliance cost for the credit institution.~~		
2. Rights granted under paragraph 1 to agents or distributors shall be granted exclusively for the provision of payment services on behalf of the payment institution.	3. Rights granted under paragraph 1 to agents ~~or distributors~~ shall be granted exclusively for the provision of payment services on behalf of the payment institution.		
3. A credit institution shall notify to the payment institution or to its agents or distributors, or to the applicant for a license as a payment institution, any decision to refuse to open or to close a payment account to a payment institution or to its agents or distributors, or to an applicant for a license as a payment institution; it shall duly motivate any such decision. Such motivation must be specific to the risks posed by the activity or planned activity of that payment institution or of its agents or distributors, as assessed by	4. ~~A~~ Without undue delay and at the latest one month after receiving an application, a credit institution shall notify to the payment institution or to its agents ~~or distributors~~, or to the applicant for a license as a payment institution, any decision to refuse to open or to close a payment account to a payment institution or to its agents ~~or distributors~~, or to an applicant for a license as a payment institution; it shall duly motivate any such decision. Such motivation must	4. ~~A~~ Without undue delay and at the latest one month after receiving an application, a credit institution shall notify to the payment institution or to its agents ~~or distributors~~, or to the applicant for a license as a payment institution, any decision to refuse to open ~~or to close~~ a payment account to a payment institution or to its agents ~~or distributors~~, or	

PUBLIC

the credit institution, and not be generic in nature.	be specific to the risks posed by the activity or planned activity of that payment institution or of its agents ~~or distributors~~, as assessed by the credit institution, based upon grounds referred to in paragraph 1 and not be generic in nature. Without prejudice to Article 21 of Regulation (EU) …/… of the European Parliament and of the Council[39], the credit institution shall notify to the payment institution or to its agents of the decision to close the payment account at least 3 months before closing the payment account. Any decision to close a payment account shall be duly motivated,	to an applicant for a license as a payment institution; it shall duly motivate any such decision. Such motivation must be specific to the risks posed by the activity or planned activity of that payment institution or of its agents ~~or distributors~~, as assessed by the credit institution, based upon grounds referred to in paragraph ~~2~~1 and not be generic in nature. Without prejudice to Article 21 of Regulation (EU) …/… of the European Parliament and of the Council[41], the	

[39] OP: Please insert in the text the number of the Regulation contained in document 2021/0239(COD) (Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - COM/2021/420 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.

[41] OP: Please insert in the text the number of the Regulation contained in document 2021/0239(COD) (Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - COM/2021/420 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.

PUBLIC

	specific and based upon grounds referred to in paragraph 1. By way of derogation from the first and second subparagraph, in the cases covered under paragraph 2~~1~~, point (a), credit institutions shall only notify to the payment institution, its agents or the applicant for a license as a payment institution that the opening or closing of an account would result in an infringement of Regulation[40] and shall not disclose any detail on the nature of that infringement.	credit institution shall notify to the payment institution or to its agents of the decision to close the payment account at least 3 months before closing the payment account. Any decision to close a payment account shall be duly motivated, specific and based upon grounds referred to in paragraph 1. By way of derogation from the first and second subparagraph, in the cases covered under paragraph 2~~1~~, point (a), credit institutions shall only notify to the payment institution, its agents or the applicant for a	

[40] OP: Please insert in the text the number of the Regulation contained in document 2021/0239(COD) (Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - COM/2021/420 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.

		license as a payment institution that the opening or closing of an account would result in an infringement of Regulation[42] and shall not disclose any detail on the nature of that infringement. *[**PRES comment**: Proposal aiming to solve inconsistencies indicated by some Member States.]*	
	5. The closure of the payment account must take into account the payment institution's ability to comply with its safeguarding duties as set out in Article 9 of Directive (EU) [PSD3].		
4. A payment institution or its agents or distributors, or an applicant for a license as a payment institution which is the subject of a	6. A payment institution or its agents ~~or distributors,~~ or an applicant for a license as a payment institution		

[42] OP: Please insert in the text the number of the Regulation contained in document 2021/0239(COD) (Proposal for a regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing - COM/2021/420 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.

PUBLIC

negative decision by a credit institution on access or of a decision on closure from payment accounts services may appeal to a competent authority.	which is the subject of a negative decision by a credit institution on access or of a decision on closure from payment accounts services may appeal to a competent authority.		
	7. Each year the credit institution shall send information to its competent authority on the number of payment accounts opened, the number of refusals and closures of payment accounts and the grounds of refusal or closure as referred to in paragraph one.	7. ~~Each year the c~~Credit institutions shall ~~send~~ provide to the competent authority on an annual basis information ~~to its competent authority~~ on the number of payment accounts opened, the number of refusals and closures of payment accounts and the grounds of refusal or closure as referred to in paragraph two~~one~~. *[**PRES comment**: Alignment of PSR wording.]*	
5. The EBA shall develop draft regulatory technical standards specifying the harmonised format and information to be contained in the notification and motivation referred to in paragraph 3 of this Article.	8. The EBA shall develop draft regulatory technical standards specifying the harmonised format and information to be contained in the notification and motivation referred to in paragraph 4 of this Article.	8. The EBA shall develop draft regulatory technical standards specifying the harmonised format and information to be contained in the notification and	

	The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010. In order to ensure the sound application of the grounds referred to in paragraph 1, the EBA shall issue guidelines on 'substantive breach of contract' pursuant to Article 16 of Regulation No 1093/2010 by 18 March 2024~~5~~.	motivation referred to in paragraph 4 of this Article. The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010. ~~In order~~ With a view to enhancing ~~ensure~~ the sound application of the grounds referred to in paragraph 2~~1~~, the EBA shall issue guidelines on 'substantive breach of contract' pursuant to Article 16 of Regulation	

		No 1093/2010 by 18 March 2024~~+~~5. ***[PRES comment**: Technical amendment.]*	
The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.	~~The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.~~The EBA shall develop draft implementing technical standards specifying the harmonised format of the report referred to in paragraph 7. The EBA shall submit the draft implementing technical standards referred to ~~in the fourth seventh sub~~paragraph 7 to the Commission by [OP please insert the date= one year after the date of entry into force of	~~The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.~~The EBA shall develop draft implementing technical standards establishing a standard ~~specifying the harmonised~~ format ~~o~~for the report containing the information to be submitted by the credit	

	this Regulation]. Power is delegated to the Commission to adopt the implementing technical standards referred to ~~in the fourth seventh sub~~paragraph 7 in accordance with Articles 15 of Regulation (EU) No 1093/2010. In order to ensure the proper application of the determination of insufficient documentation in terms of the access of payment account for payment institutions, its agents and applicants referred to in paragraph 1 point c, the EBA shall submit draft regulatory technical standards, *after consultation with AMLA.*	institutions to the competent authorities as referred to in paragraph 7. The EBA shall submit the draft implementing technical standards referred to ~~in the fourth seventh sub~~paragraph 7 to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the implementing technical standards referred to ~~in the fourth seventh sub~~paragraph 7 in accordance with Articles 15 of Regulation (EU) No 1093/2010. In order to specify the rules for ~~ensure the proper application of the determination~~ determining ~~of~~ insufficient documentation in terms of the access of payment account for payment institutions, its	

		agents and applicants referred to in paragraph 1 point c, the EBA shall submit draft regulatory technical standards, *after consultation with AMLA*. The EBA shall submit these draft regulatory technical standards to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010. *[**PRES comment**: Alignment with wording of Article 82(3). The standard wording on RTS has been added as it seemed to be missing.]*	

PUBLIC

	Article 32a	Article 32a	
	Virtual IBANs	**Virtual IBANs**	
	1. A virtual IBAN as defined in Article 2(20c) of Regulation (EU) No. XXX [AML Regulation] is to be considered as an IBAN as defined in Article 2(15) of Regulation (EU) No 260/2012 [SEPA].	1. A virtual IBAN as defined in Article 2(20c) of Regulation (EU) No. XXX [AML Regulation] is to be considered as an IBAN as defined in Article 2(15) of Regulation (EU) No 260/2012 [SEPA].	
	2. The country code of the virtual IBAN as defined in Article 2(20c) of Regulation (EU) No. XXX [AML Regulation] shall always match the country code of the payment account to which it causes payments to be redirected.	~~2. The country code of the virtual IBAN as defined in Article 2(20c) of Regulation (EU) No. XXX [AML Regulation] shall always match the country code of the payment account to which it causes payments to be redirected.~~ ***[PRES comment:** The proposal presented at the February CWP meeting.]*	
Chapter 3			

PUBLIC

Account information services and payment initiation services			
Section 1			
General Principles			
Article 33			
Rights of payment service users			
1. Payment service providers shall not prevent payment service users from making use of a payment initiation service provider to obtain payment initiation services as referred to in point (6) of Annex I. That obligation shall apply to all the payment accounts held by the payment service user that are accessible online.		1. Payment service providers shall not prevent payment service users from making use of a payment initiation service provider to obtain payment initiation services as referred to in point (6) of Annex I to Directive XXX [PSD3]. That obligation shall apply to all the payment accounts held by the payment service user that are accessible online. ***[PRES comment**: The alignment with the approach taken under the Hungarian Presidency to remove Annex I from the PSR and maintain*	

		the Annex on payment services only in PSD3.]	
2. Payment service providers shall not prevent payment service users from making use of account information services as referred to in point (7) of Annex I. That obligation shall apply to all the payment accounts held by the payment service user that are accessible online.		2. Payment service providers shall not prevent payment service users from making use of account information services as referred to in point (7) of Annex I to Directive XXX [PSD3]. That obligation shall apply to all the payment accounts held by the payment service user that are accessible online. *[**PRES comment**: The alignment with the approach taken under the Hungarian Presidency to remove Annex I from the PSR and maintain the Annex on payment services only in PSD3.]*	
Article 34			
Contractual relations			

PUBLIC

1. The provision of account information services and payment initiation services shall not be conditioned by any party on the existence of a contractual relationship to that end between providers of such services and an account servicing payment service provider.			
2. Where a multilateral contractual arrangement is in place and where the same payment account data as regulated under this Regulation is also available in the framework of that multilateral contractual arrangement, access by account information and payment initiation service providers to payment account data regulated under this Regulation shall always be possible without the need to be part of such multilateral contractual arrangement.			
Section 2			
Data access interfaces for account information services and payment initiation services			
Article 35			
Provision of dedicated access interfaces			

PUBLIC

1. Account servicing payment service providers that offer to a payer a payment account that is accessible online shall have in place at least one dedicated interface for the purpose of data exchange with account information and payment initiation service providers.			
2. Without prejudice to Articles 38 and 39, account servicing payment service providers that offer to a payer a payment account that is accessible online and have put in place a dedicated interface as referred to in paragraph 1 of this Article, shall not be obliged to also maintain permanently another interface as fall-back for the purpose of data exchange with account information and payment initiation service providers.	2. Account servicing payment service providers shall put in place their dedicated interface within three months of obtaining their license. ~~Without prejudice to Articles 38 and 39, account servicing payment service providers that offer to a payer a payment account that is accessible online and have put in place a dedicated interface as referred to in paragraph 1 of this Article, shall not be obliged to also maintain permanently another interface as fall-back for the purpose of data exchange with account information and payment initiation service providers.~~ The account servicing payment service provider is obligated to provide the relevant technical	2. Account servicing payment service providers shall put in place their dedicated interface within three months of obtaining their license. ~~Without prejudice to Articles 38 and 39, account servicing payment service providers that offer to a payer a payment account that is accessible online and have put in place a dedicated interface as referred to in paragraph 1 of this Article, shall not be obliged to also maintain permanently another interface as fall-back for the purpose of data~~	

	documentation of the dedicated interface in a timely manner, such that third-party payment service providers can use the dedicated interface as soon as possible.	~~exchange with account information and payment initiation service providers~~. The account servicing payment service provider ~~is obligated to~~shall provide the relevant technical documentation of the dedicated interface without undue delay in a timely manner, upon request by authorised payment initiation service providers, account information service providers or by payment service providers that have applied to their competent authorities for the relevant authorisation so ~~such~~ that third-party payment service providers can use the dedicated interface as soon as possible. *[**PRES comment**: The proposal presented at the January CWP meeting. The*	

		purpose of this amendment is the alignment with the followig paragraph.]	
3. Account servicing payment service providers shall ensure that their dedicated interfaces referred to in paragraph 1 use standards of communication which are issued by European or international standardisation organisations including the European Committee for Standardization (CEN) or the International Organization for Standardization (ISO). Account servicing payment service providers shall also ensure that the technical specifications of any of the dedicated interfaces referred to in paragraph 1 are documented specifying a set of routines, protocols and tools needed by payment initiation service providers and account information service providers for allowing their software and applications to interoperate with the systems of the account servicing payment service provider. Account servicing payment service providers shall make the documentation on technical specifications of their dedicated interfaces referred to in paragraph 1 available, at no	3. Account servicing payment service providers shall ensure that their dedicated interfaces referred to in paragraph 1 use standards of communication which are issued by European or international standardisation organisations including the European Committee for Standardization (CEN) or the International Organization for Standardization (ISO) or other relevant standards. Account servicing payment service providers shall also ensure that the technical specifications of any of the dedicated interfaces referred to in paragraph 1 are documented specifying a set of routines, protocols and tools needed by payment initiation service providers and account information service providers for allowing their software		

PUBLIC

charge and without delay, upon request by authorised payment initiation service providers, account information service providers or by payment service providers that have applied to their competent authorities for the relevant authorisation and shall make a summary of that documentation publicly available on their website.	and applications to interoperate with the systems of the account servicing payment service provider. Account servicing payment service providers shall make the documentation on technical specifications of their dedicated interfaces referred to in paragraph 1 available, ~~at no~~ free of charge and without undue delay, upon request by authorised payment initiation service providers, account information service providers or by payment service providers that have applied to their competent authorities for the relevant authorisation and shall make a summary of that documentation publicly available on their website.		
4. Account servicing payment service providers shall ensure that, except for emergency situations which prevent them from doing so, any change to the technical specifications of their dedicated interface referred to in paragraph 1 is made available to authorised payment initiation service providers, account information service	4. Account servicing payment service providers shall ensure that, except for emergency situations which prevent them from doing so, any change to the technical specifications of their dedicated interface referred to in paragraph 1 is made available, as a minimum through publication on		

PUBLIC

providers, or payment service providers that have applied to their competent authorities for the relevant authorisation, in advance, as soon as possible and not less than 3 months before the change is implemented. Account servicing payment service providers shall document emergency situations where changes were implemented without such advance information and make the documentation available to competent authorities on request.	their website, to authorised payment initiation service providers, account information service providers, or payment service providers that have applied to their competent authorities for the relevant authorisation, in advance, as soon as possible and not less than 3 months before the change is implemented. Account servicing payment service providers shall document emergency situations where changes were implemented without such advance information and make the documentation available to competent authorities on request.		
5. Account servicing payment service providers shall publish on their website quarterly statistics on the availability and performance of their dedicated interface. The performance of the dedicated interfaces shall be measured by the number of successful account information requests over the total number of account information requests, and by the number and transaction volume of the successful payment initiation requests over	5. Account servicing payment service providers shall publish on their website quarterly statistics on the availability, unplanned unavailability and performance of their dedicated interface, and, for comparison purposes, of the interfaces that the account servicing payment service provider makes available to its payment service users for directly		

PUBLIC

the total number and transaction volume of the total number of payment initiation requests.	accessing their payment account online. The performance of the dedicated interfaces shall be measured by the number of successful account information requests over the total number of account information requests, and by the number and transaction volume of the successful payment initiation requests over the total number and transaction volume of the total number of payment initiation requests.		
6. Account servicing payment service providers shall make available a testing facility, including support, for connection to the dedicated interfaces and functional testing to enable authorised payment initiation service providers and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users. No sensitive payment data or any other personal data shall be shared through the testing facility.			

PUBLIC

7. In case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements via the dedicated interface, the account servicing payment service provider shall provide for notification messages to the payment initiation service provider or the account information service provider which explains the reason for the unexpected event or error.			
Article 36			
Requirements regarding dedicated data access interfaces			
1. Account servicing payment service providers shall ensure that the dedicated interface referred to in Article 35(1) meets the following security and performance requirements:			
(a) the dedicated interface shall establish and maintain communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and any payment service			

PUBLIC

user concerned throughout the authentication of the payment service user;			
(b) the dedicated interface shall ensure the integrity and confidentiality of the personalised security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider;			
(c) the response time of the dedicated interface to account information service providers' and payment initiation service providers' access requests shall not be longer than the response time of the interface that the account servicing payment service provider makes available to its payment service users for directly accessing their payment account online.			
2. Account servicing payment service providers shall ensure that the dedicated interface referred to in Article 35(1) allows both account information service providers and payment initiation service providers to:			
(a) identify themselves towards the account servicing payment service provider;			

PUBLIC

(b) instruct the account servicing payment service provider to start the authentication based on the permission of the payment service user given to the account information service provider or the payment initiation service providers in accordance with Article 49(2);			
(c) make use, in a non-discriminatory manner, of any authentication exemptions applied by the account servicing payment service provider;			
(d) see, prior to initiation of the payment in the case of payment initiation service providers, the unique identifier of the account, the associated names of the account holder and the currencies as available to the payment service user.			
3. Account servicing payment service providers shall allow account information service providers to communicate securely, via the dedicated interface, to request and receive information on one or more designated payment accounts and associated payment transactions.	3. Account servicing payment service providers shall allow account information service providers to communicate securely, via the dedicated interface, to request and receive information on one or more designated payment accounts and associated payment transactions. <u>This includes payment transactions</u>	3. Account servicing payment service providers shall allow account information service providers to communicate securely, via the dedicated interface, to request and receive information on one or more designated payment	

	initiated through a payment instrument which have not yet been charged to the payment account, if these transactions are already visible in the customer interface.	accounts and associated payment transactions. ~~This includes payment transactions initiated through a payment instrument which have not yet been charged to the payment account, if these transactions are already visible in the customer interface~~. *[**PRES comment**: In view of the PRES, there were diverging views as regards interpretation of this sentence. Therefore it is proposed to delete this sentence. If MSs decide to keep this sentence it should be clarified, including in the recitals, what this provision intends to achieve, so that the understanding of the proposed amendment is clear and unambiguous.]*	
4. Account servicing payment service providers shall ensure that the dedicated			

PUBLIC

interface allows payment initiation service providers, at a minimum, to:			
(a) place and revoke a standing payment order or a direct debit;	(a) place and revoke a standing payment order ~~or a direct debit~~;		
(b) initiate a single payment;			
(c) initiate and revoke a future dated payment;			
(d) initiate payments to multiple beneficiaries;			
(e) initiate payments, regardless of whether the payee is on the payer's beneficiaries list;	(e) initiate payments, regardless of whether the payee is on the payer's beneficiaries list provided the payment service user has the ability to perform these in the interface that the account servicing payment service provider uses for authentication and communication with its users;	(e) initiate payments, regardless of whether the payee is on the payer's beneficiaries list provided that the payment service user has the ability to perform these payments in the interface that the account servicing payment service provider uses for authentication and communication with its users; *[**PRES comment**: Technical amendment.]*	
(f) communicate securely to place a payment order from the payer's payment			

PUBLIC

account and receive all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction;			
(g) verify the name of the account holder before the payment is initiated and regardless of whether the name of the account holder is available via the direct interface;			
(h) initiate a payment with one single strong customer authentication, provided the payment initiation service provider has provided the account servicing payment service provider with all of the following:	~~(h) initiate a payment with one single strong customer authentication, provided the payment initiation service provider has provided the account servicing payment service provider with all of the following~~		
(i) the payer's unique identifier,	~~(i) the payer's unique identifier~~		
(ii) the payee's legal and commercial name and 'unique identifier',	~~(ii) the payee's legal and commercial name and 'unique identifier',~~		
(iii) a transaction reference,	~~(iii) a transaction reference,~~		
(iv) the payment amount and the currency of the payment, based on which the single strong customer authentication is triggered.	~~(iv) the payment amount and the currency of the payment, based on which the single strong customer authentication is triggered.~~		
5. Account servicing payment service providers shall ensure that the dedicated			

PUBLIC

interface provides to payment initiation service providers:			
(a) the immediate confirmation, upon request, in a simple 'yes' or 'no' format, of whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer;			
(b) the confirmation from the account servicing payment service provider that the payment will be executed on the basis of the information available to the account servicing payment service provider, taking into account any pre-existing payment orders that might affect the full execution of the payment order being placed.			
The information referred to in point (b) shall not be shared with the payment initiation service provider but may be used by the account servicing payment service provider in order to provide confirmation of the execution of the operation.			
	6. For the activities of payment initiation services and account information services the name and the account number of the account		

PUBLIC

	owner shall not constitute sensitive payment data.		
Article 37			
Data access parity between dedicated access interface and customer interface			
1. Without prejudice to Article 36, account servicing payment service providers shall ensure that their dedicated interface referred to in Article 35(1) offers at all times at least the same level of availability and performance, including technical and IT support, as the interfaces that account servicing payment service providers make available to the payment service user for directly accessing its payment account online.			
2. Account servicing payment service providers shall provide account information services providers with at least the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this			

PUBLIC

information does not include sensitive payment data.			
3. Account servicing payment service providers shall provide payment initiation service providers with at least the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the payment service user. That information shall be provided immediately after receipt of the payment order and on an ongoing basis until the payment is final.	3. Account servicing payment service providers shall provide payment initiation service providers with at least the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the payment service user. That information shall be provided immediately after receipt of the payment order and be made available to payment initation service providers to access on an ongoing basis until the payment is final.		
Article 38			
Contingency measures for an unavailable dedicated interface	**~~Contingency measures for an unavailable dedicated interface~~ Availability and performance requirements for the dedicated interface**		

PUBLIC

1. Account servicing payment service providers shall take all measures in their power to prevent unavailability of the dedicated interface. Unavailability shall be presumed to have arisen when five consecutive requests for access to information for the provision of payment initiation services or account information services receive no response from the account servicing payment service provider's dedicated interface within 30 seconds.	1. Account servicing payment service providers shall take all measures in their power to prevent unplanned unavailability of the dedicated interface. Unplanned unavailability shall be presumed to have arisen when five consecutive requests for access to information for the provision of payment initiation services or account information services receive no response or server error responses from the account servicing payment service provider's dedicated interface within 30 seconds.		
2. In case of unavailability of the dedicated interface, account servicing payment service providers shall inform payment service providers making use of the dedicated interface of measures taken to restore the interface and of the time estimated necessary for the problem to be resolved. During the period of unavailability, account servicing payment service providers shall offer to account information and payment initiation service providers without delay an	2. In case of planned unavailability of the dedicated interface, account servicing payment service providers shall as a rule, except for emergency changes, inform payment service providers making use of the dedicated interface at least one month in advance of the planned unavailability and its duration. Planned unavailability shall normally occur between 00:00 and 06:00. ~~of~~		

PUBLIC

effective alternative solution, such as the use of the interface that the account servicing payment service provider uses for authentication and communication with its users, to access payment account data.	~~measures taken to restore the interface and of the time estimated necessary for the problem to be resolved. During the period of unavailability, account servicing payment service providers shall offer to account information and payment initiation service providers without delay an effective alternative solution, such as the use of the interface that the account servicing payment service provider uses for authentication and communication with its users, to access payment account data.~~		
3. Where the dedicated interface is unavailable and the account servicing payment service provider has not offered a rapid and effective alternative solution referred to in paragraph 2, payment initiation service providers or account information service providers may request their competent authority, providing all necessary information and evidence, to allow them to use the interface that the account servicing payment service provider uses for	3. In case of unplanned unavailability of the dedicated interface, account servicing payment service providers shall timely inform payment initiation service providers and account information service providers ~~payment service providers~~ making use of the dedicated interface of measures taken to restore the interface and of the time estimated necessary for the problem to be	3. In case of unplanned unavailability of the dedicated interface, account servicing payment service providers shall timely inform payment initiation service providers and account information service providers ~~payment service providers~~ making use of the dedicated interface of	

authentication and communication with its users for payment account data access.	resolved. They shall ensure an optimal recovery time of the dedicated interface. ~~Where the dedicated interface is unavailable and the account servicing payment service provider has not offered a rapid and effective alternative solution referred to in paragraph 2, payment initiation service providers or account information service providers may request their competent authority, providing all necessary information and evidence, to allow them to use the interface that the account servicing payment service provider uses for authentication and communication with its users for payment account data access.~~	measures taken to restore the interface and of the time estimated necessary for the problem to be resolved. ~~They~~ Account servicing payment service providers shall ensure an optimal recovery time of the dedicated interface. ~~Where the dedicated interface is unavailable and the account servicing payment service provider has not offered a rapid and effective alternative solution referred to in paragraph 2, payment initiation service providers or account information service providers may request their competent authority, providing all necessary information and evidence, to allow them to use the interface that the account servicing payment service~~	

PUBLIC

		~~provider uses for authentication and communication with its users for payment account data access.~~ *[**PRES comment**: Technical amendment.]*	
4. Based on the request referred to in paragraph 3, the competent authority may for a time-limited period until the dedicated interface is restored to availability, authorise all payment initiation service providers and account information service providers to access payment accounts data via an interface that the account servicing payment service provider uses for authentication and communication with its users. The competent authority shall communicate its decision to the requesting account information service provider or payment initiation service provider and make it publicly available on its website. The competent authority shall instruct the account servicing payment service provider to restore the full functioning of the dedicated interface before the expiry of the temporary authorisation.	4. The account servicing payment service providers shall ensure that the dedicated interface provides ~~shall ensure~~ an availability and performance that equals at least that of the interface that the account servicing payment service provider uses for authentication and communication with its users. ~~Based on the request referred to in paragraph 3, the competent authority may for a time-limited period until the dedicated interface is restored to availability, authorise all payment initiation service providers and account information service providers to access payment accounts data via an interface that the account servicing payment service provider~~		

PUBLIC

	~~uses for authentication and communication with its users. The competent authority shall communicate its decision to the requesting account information service provider or payment initiation service provider and make it publicly available on its website. The competent authority shall instruct the account servicing payment service provider to restore the full functioning of the dedicated interface before the expiry of the temporary authorisation.~~		
5. The competent authority shall take a decision without undue delay on any request introduced under paragraph 3. As long as the competent authority has not taken a decision on the request, the requesting payment initiation service provider or account information service provider may exceptionally access payment accounts data via an interface that the account servicing payment service provider uses for authentication and communication with its users. The requesting payment initiation	~~5. The competent authority shall take a decision without undue delay on any request introduced under paragraph 3. As long as the competent authority has not taken a decision on the request, the requesting payment initiation service provider or account information service provider may exceptionally access payment accounts data via an interface that the account servicing payment service provider uses for~~		

PUBLIC

service provider or account information service provider shall cease to do so when the dedicated interface is restored to availability, or when the competent authority adopts a decision not authorising such use, whichever is the sooner.	~~authentication and communication with its users. The requesting payment initiation service provider or account information service provider shall cease to do so when the dedicated interface is restored to availability, or when the competent authority adopts a decision not authorising such use, whichever is the sooner.~~		
6. In cases where account servicing payment service providers are obliged to allow account information service providers or payment initiation service providers to access the interface that account servicing payment service providers use for authentication and communication with their users, account servicing payment service providers shall immediately make available any technical specifications needed by account information service providers or payment initiation service providers to adequately connect to the interface that the account servicing payment service provider uses for authentication and communication with its users.	5. The EBA shall develop draft regulatory technical standards which shall specify: (a) the requirements related to the quarterly statistics on the availability and performance of ~~dedicated~~ the interfaces referred to in paragraph 5 of Article 35 and the publication thereof ; (b) the standards establishing an optimal recovery time in case of dedicated interface unplanned unavailability pursuant to paragraph 3, based on the severity of the incident.		

PUBLIC

	For the purposes of point (b), the severity shall take into account, among others, the number of customers impacted and types of functionality affected of account information and payment initiation service providers. The EBA shall submit the draft regulatory technical standards referred to in this paragraph to the Commission by [(date here, e.g.:) "OP please insert the date = one year after the date of entry into force of this Regulation"]. Power is delegated to the Commission to adopt these regulatory technical standards in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010. ~~6. In cases where account servicing payment service providers are obliged to allow account information service providers or payment initiation service providers to access the interface that account servicing payment service providers use for~~		

PUBLIC

	~~authentication and communication with their users, account servicing payment service providers shall immediately make available any technical specifications needed by account information service providers or payment initiation service providers to adequately connect to the interface that the account servicing payment service provider uses for authentication and communication with its users.~~		
7. When accessing the interface that the account servicing payment service provider uses for authentication and communication with its users, the account information service providers or payment initiation service providers shall meet all requirements laid down in Article 45(2). In particular, the account information service providers or payment initiation service providers shall always duly identify themselves with the account servicing payment services provider.	~~7. When accessing the interface that the account servicing payment service provider uses for authentication and communication with its users, the account information service providers or payment initiation service providers shall meet all requirements laid down in Article 45(2). In particular, the account information service providers or payment initiation service providers shall always duly identify themselves with the account servicing payment services provider.~~		

PUBLIC

Article 39			
Derogation from having a dedicated interface for data access			
1. By way of derogation from Article 35(1), on request of an account servicing payment service provider, the competent authority may exempt the requesting account servicing payment service provider from the obligation to have in place a dedicated interface and allow the account servicing payment service provider to either offer, as interface for secure data exchange, one of the interfaces that the account servicing payment service provider uses for authentication and communication with its payment services users or, where justified, not to offer any interface at all for secure data exchange.	1. By way of derogation from Article 35(1), on request of an account servicing payment service provider, the competent authority may exempt the requesting account servicing payment service provider from the obligation to have in place a dedicated interface and allow the account servicing payment service provider to either offer, as interface for secure data exchange, ~~one of~~ the interfaces that the account servicing payment service provider uses for authentication and communication with its payment service~~s~~ users provided this interface is an API endpoint or, where justified, not to offer any interface at all for secure data exchange.	1. By way of derogation from Article 35(1), on request of an account servicing payment service provider, the Member State or the competent authority may exempt the requesting account servicing payment service provider from the obligation to have in place a dedicated interface and allow the account servicing payment service provider to either offer, as interface for secure data exchange, ~~one of~~ the interfaces that the account servicing payment service provider uses for authentication and communication with its payment service~~s~~ users	

		provided this interface is an API endpoint or, where justified, not to offer any interface at all for secure data exchange. ***[PRES comment:*** *Amendments based on the non-paper of one of the Member States reflecting specific national cirucmstances.]*	
2. The EBA shall develop draft regulatory technical standards which shall specify the criteria on the basis of which, in accordance with paragraph 1, an account servicing payment service provider may be exempted from the obligation to have in place a dedicated interface and be allowed either to provide, as interface for secure data exchange with account information service providers and payment initiation service providers, the interface that it makes available to its payment user for accessing its payment accounts online or, where appropriate, not to have any interface at all for secure data exchange.	2. The EBA shall develop draft regulatory technical standards which shall specify the criteria on the basis of which, in accordance with paragraph 1, an account servicing payment service provider may be exempted from the obligation to ~~have in place a dedicated interface~~ offer any interface at all for secure data exchange. When developing these criteria, the EBA shall, inter alia, consider the size, annual turnover and payments volume of the account servicing payment service provider. ~~and be allowed either to provide, as~~		

PUBLIC

	~~interface for secure data exchange with account information service providers and payment initiation service providers, the interface that it makes available to its payment user for accessing its payment accounts online or, where appropriate, not to have any interface at all for secure data exchange.~~		
The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by [OP please insert the date= one year after the date of entry into force of this Regulation]. Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.			
Section 3			
Rights and obligations of account servicing payment services providers			
Article 40			

PUBLIC

Obligations on account servicing payment service providers regarding payment initiation services			
The account servicing payment service provider shall perform the following actions to ensure the payer's right to use the payment initiation service:			
(a) communicate securely with payment initiation service providers;			
(b) immediately after receipt of the payment order from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider;		(b) immediately after receipt of the payment order from a payment initiation service provider, ~~provide or~~ make available on an ongoing basis all information on the initiation of the payment transaction and all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider; ***[PRES comment:*** *Amendments as requested by*	

		one of the Member States to clarify that information should be made available on an ongoing basis. The MS also argue that 'providing' such information in a meaning to 'push' it is practically impossible.]	
(c) treat payment orders transmitted through the services of a payment initiation service provider as if those payment orders were payment orders transmitted directly by the payer or the payee, in particular in terms of timing, priority or charges.	(c) treat payment orders transmitted through the services of a payment initiation service provider as if those payment orders were payment orders transmitted directly by the payer or the payee, in particular in terms of timing, priority or charges and without any discrimination.		
For the purposes of point (b), where some or all of the information referred to in that point is unavailable immediately after receipt of the payment order, the account servicing payment service provider shall ensure that any information about the execution of the payment order is made available to the payment initiation service provider immediately after that information becomes			

PUBLIC

available to the account servicing payment service provider.			
Article 41			
Obligations of account servicing payment service providers regarding account information services			
1. The account servicing payment service provider shall perform the following actions to ensure the payment service user's right to use the account information service:			
(a) communicate securely with the account information service provider;			
(b) treat data requests transmitted through the services of an account information service provider as if the data were requested by the payment service user via the interface that the account servicing payment service provider makes available to its payment service users for directly accessing their payment account.	(b) treat data requests transmitted through the services of an account information service provider as if the data were requested by the payment service user via the interface that the account servicing payment service provider makes available to its payment service users for directly accessing their payment account <u>and without any discrimination</u>.		
2. Account servicing payment service providers shall allow account information			

PUBLIC

service providers to access information from designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of performing the account information service whether or not the payment service user is actively requesting such information.			
	3. The account information service provider shall ensure that the payment service user is duly aware of its intent to access information as per paragraph 2 of this Article when the payment service user is not actively requesting such information. It shall inform the payment service user thereof before making use of this functionality.		
Article 42			
Restriction of access to payment accounts by account information service providers and payment initiation service providers			
1. An account servicing payment service provider may deny an account			

PUBLIC

information service provider or a payment initiation service provider access to a payment account for objectively justified and duly evidenced reasons. Those reasons shall relate to unauthorised, as per Article 49(3), or fraudulent access to the payment account by that account information service provider or that payment initiation service provider, including the unauthorised or fraudulent initiation of a payment transaction. In such cases, the account servicing payment service provider shall inform the payment services user that access to the payment account is denied and provide the reasons therefor. That information shall, where possible, be provided to the payment services user before access is denied and at the latest immediately thereafter, unless providing such information would compromise objectively justified security reasons or is prohibited by other relevant Union or national law.			
2. In the cases referred to in paragraph 1, the account servicing payment service provider shall immediately report the incident relating to the account information service provider or the payment initiation			

PUBLIC

service provider to the competent authority. The information shall include the relevant details of the case and the reasons for taking action. The competent authority shall assess the case and shall, if necessary, take appropriate measures.			
Article 43			
Data access management by payment service users			
1. The account servicing payment service provider shall provide the payment service user with a dashboard, integrated into its user interface, to monitor and manage the permissions the payment service user has given for the purpose of account information services or payment initiation services covering multiple or recurrent payments.			
2. The dashboard shall:			
(a) provide the payment service user with an overview of each ongoing permission given for the purposes of account information services or payment initiation services, including:		(a) provide the payment service user with an overview of each ongoing permission given for the purposes of account information services or	

PUBLIC

		payment initiation services at any time, including:	
(i) the name of the account information service provider or payment initiation service provider to which access has been granted;			
(ii) the customer account to which access has been granted;			
(iii) the purpose of the permission;			
(iv) the period of validity of the permission;		(iv) the period of validity of the permission, including the date on which the payment service user has given their permission, and the dates on which a payment account was accessed;	
(v) the categories of data being shared.			
(b) allow the payment service user to withdraw data access for a given account information service or payment initiation service provider;		(b) allow the payment service user to withdraw data access for a given account information service or payment initiation service provider at any time;	
(c) allow the payment service user to re-establish any data access withdrawn;	(c) allow the payment service user to re-establish any data access withdrawn up to 48 hours after withdrawal of this data access;	(c) within 48 hours from withdrawal of a permission, allow the payment service user to re-establish any data	

		access withdrawn ~~up to 48 hours after withdrawal of this data access~~;	
(d) include a record of data access permissions that have been withdrawn or have expired, for a duration of two years.			
	(e) be consistent with the Regulation (EU) [..../....] of the European Parliament and of the Council [FIDA] dashboards and allow payment service users to manage data permissions pursuant to this Regulation and [FIDA] through a single dashboard upon the request of the payment service user.		
	Where, pursuant to paragraph 2, point (b), a payment service user decides to withdraw data access, the payment initation service provider or account information service provider concerned shall: (a) cease using the data; (b) withdraw the data; and (c) without undue delay, erase all data received as a result of the data	2a. Where, pursuant to paragraph 2, point (b), a payment service user decides to withdraw data access, the payment initation service provider or account information service provider concerned shall: (a) cease using the data;	

	access permission granted by the payment service user.	~~(b) withdraw the data; and~~ (c) without undue delay, erase all data received as a result of the data access permission granted by the payment service user.	
3. The account servicing payment service provider shall ensure that the dashboard is easy to find in its user interface and that information displayed on the dashboard is clear, accurate and easily understandable for the payment service user.	3. The account servicing payment service provider shall ensure that the dashboard is easy to find in its user interface and that information displayed on the dashboard is clear, accurate and easily understandable for the payment service user and does not contain any deterring or discouraging language that might dissuade the payment service user from making use of the services of a payment initiation service provider or account information service provider.	3. The account servicing payment service provider shall ensure that the dashboard is easy to find in its user interface and that information displayed on the dashboard is clear, neutral accurate and easily understandable for the payment service user and does not contain any deterring or discouraging language that might dissuade the payment service user from making use of the services of a payment initiation service provider or account information service provider.	

4. The account servicing payment service provider and the account information service or payment initiation service provider to which permission has been granted shall cooperate to make information available to the payment service user via the dashboard in real-time. For the purposes of paragraph 2 points (a), (b), (c) and (e):	4. The ~~account servicing payment service provider and the~~ account information service or payment initiation service provider to which permission has been granted shall provide the information in paragraph 2 point (a) to the account servicing payment service provider as soon as possible and within 24 hours from the permission being granted. The account servicing payment service provider shall only provide the information in paragraph 2 point (a) to the extent it was provided to it by the account information service or payment initiation service provider to which permission has been granted. ~~cooperate to make information available to the payment service user via the dashboard in real-time. For the purposes of paragraph 2 points (a), (b), (c) and (e):~~	4. The ~~account servicing payment service provider and the~~ account information service or payment initiation service provider to which permission has been granted shall provide the information in paragraph 2 point (a) to the account servicing payment service provider in real time ~~as soon as possible and within 24 hours from the permission being granted~~. The account servicing payment service provider shall only provide the information in paragraph 2 point (a) to the extent it was provided to it by the account information service or payment initiation service provider to which permission has been granted. ~~cooperate to make information available to the payment service user via the dashboard in real-time. For~~	

PUBLIC

		~~the purposes of paragraph 2 points (a), (b), (c) and (e):~~	
(a) The account servicing payment service provider shall inform the account information service or payment initiation service provider in real time of changes made to a permission concerning that provider made by a payment service user via the dashboard;	~~(a) The account servicing payment service provider shall inform the account information service or payment initiation service provider in real time of changes made to a permission concerning that provider made by a payment service user via the dashboard;~~		
(b) An account information service or payment initiation service provider shall inform the account servicing payment service provider in real time of a new permission granted by a payment service user regarding a payment account provided by that account servicing payment service provider, including:	~~(b) An account information service or payment initiation service provider shall inform the account servicing payment service provider in real time of a new permission granted by a payment service user regarding a payment account provided by that account servicing payment service provider, including:~~		
(i) the purpose of the permission granted by the payment service user;	~~(i) the purpose of the permission granted by the payment service user;~~		
(ii) the period of validity of the permission;	~~(ii) the period of validity of the permission;~~		
(iii) the categories of data concerned.	~~(iii) the categories of data concerned.~~		
	5. The account servicing payment service provider and the account	5. The account servicing payment service provider	

	information service or payment initiation service provider to which permission has been granted shall cooperate to make information available to the payment service user via the dashboard as soon as possible and within 24 hours from the receipt thereof by the account servicing payment service provider pursuant to paragraph 4. For the purposes of paragraph 2 points (a), (b), (c) and (d):	and the account information service or payment initiation service provider to which permission has been granted shall cooperate to make information available to the payment service user via the dashboard without undue delay ~~as soon as possible and within 24 hours from the receipt thereof by the account servicing payment service provider pursuant to paragraph 4~~. For the purposes of paragraph 2 points (a), (b), (c) and (d) of this Article:	
	(a) The account servicing payment service provider shall inform the account information service or payment initiation service provider as soon as possible and within 24 hours at the latest of changes made to a permission concerning that	(a) The account servicing payment service provider shall ~~inform~~ notify the account information service or payment initiation service provider ~~without undue delay as soon as possible and within 24 hours at the latest~~ of any changes made by the	

	provider made by a payment service user via the dashboard;	payment service user via the dashboard to a permission, including the withdrawal of a permission;	
	(b) An account information service or payment initiation service provider shall inform the account servicing payment service provider as soon as possible and within 24 hours at the latest of a new permission granted by a payment service user regarding a payment account provided by that account servicing payment service provider, including all the information listed in paragraph 2 point (a) points (i) to (v).	(b) An account information service or payment initiation service provider shall inform the account servicing payment service provider without undue delay ~~as soon as possible and within 24 hours at the latest~~ of a new permission granted by a payment service user regarding a payment account provided by that account servicing payment service provider, including all the information listed in paragraph 2 point (a) points (i) to (v).	
	6. The account servicing payment service provider shall bear no liability for the actions envisaged in paragraph 2 points (b) and (c)	~~6. The account servicing payment service provider shall bear no liability for the actions envisaged in~~	

	undertaken by the payment service user.	~~paragraph 2 points (b) and (c) undertaken by the payment service user.~~	
Article 44			
Prohibited obstacles to data access			
1. Account servicing payment service providers shall ensure that their dedicated interface does not create obstacles to the provision of payment initiation and account information services.	~~1.~~ Account servicing payment service providers shall ensure that their dedicated interface does not create obstacles to the provision of payment initiation and account information services.		
Prohibited obstacles shall include the following:	Prohibited obstacles shall include, but not be limited to, the following:		
(a) preventing the use by payment initiation services providers or account information services providers of the credentials issued by account servicing payment service providers to their payment services users;	(a) preventing the use by payment initiation services providers or account information services providers of the personalised security credentials issued by account servicing payment service providers to their payment services users;		
(b) requiring the payment service users to manually input their unique identifier into the domain of the account servicing payment	~~(b) requiring the payment service users to manually input their unique identifier into the domain of the account servicing payment service~~		

PUBLIC

service provider to be able to use account information or payment initiation services;	~~provider to be able to use account information or payment initiation services;~~		
(c) requiring additional checks of the permission given by the payment service users to a payment initiation service provider or an account information services provider;	(~~c~~ b) requiring ~~additional~~ checks of the permission given by the payment service users to a payment initiation service provider or an account information services provider;		
(d) requiring additional registrations by payment initiation and account information services providers to be able to access the payment services user's payment account or the dedicated interface;	(~~d~~ c) without prejudice to the ability to fulfil the requirements in Article 38(2) and (3), requiring additional registrations by payment initiation and account information services providers to be able to access the payment services user's payment account or the dedicated interface;		
(e) requiring, unless indispensable to facilitate the exchange of information between account servicing payment service providers and payment initiation and account information services providers related, in particular, to the updating of the dashboard referred to in Article 43, that payment initiation and account information services providers pre-register their contact details	(~~e~~ d) requiring, unless ~~indispensable~~ necessary to facilitate the exchange of information between account servicing payment service providers and payment initiation and account information services providers related, in particular, to the updating of the dashboard referred to in Article 43, that payment initiation and account information services		

PUBLIC

with the account servicing payment service provider;	providers pre-register their contact details with the account servicing payment service provider;		
(f) restricting the possibility of a payment service user to initiate payments via a payment initiation service provider only to those payees that are on the payer's beneficiaries list;	(~~f~~ e) restricting the possibility of a payment service user to initiate payments via a payment initiation service provider only to those payees that are on the payer's beneficiaries list if such restriction does not exist in the interface that the account servicing payment service provider uses for authentication and communication with its users;		
(g) restricting payment initiations to or from domestic unique identifiers only;	(~~g~~ f) restricting payment initiations to or from domestic unique identifiers only;		
(h) requiring that strong customer authentication is applied more times in comparison with the strong customer authentication as required by the account servicing payment service provider when the payment service user is directly accessing their payment account or initiating a payment with the account servicing payment services provider;	(~~h~~ g) requiring that strong customer authentication is applied more times in comparison with the strong customer authentication as required by the account servicing payment service provider when the payment service user is directly accessing their payment account or initiating a payment with the account servicing payment services provider;		

PUBLIC

(i) providing a dedicated interface that does not support all the authentication procedures made available by the account servicing payment service provider to its payment service user;	(~~i~~ h) providing a dedicated interface that does not support all the authentication procedures made available by the account servicing payment service provider to its payment service user;		
(j) imposing an account information or payment initiation journey, in a 'redirection' or 'decoupled' approach, where the authentication of the payment service user with the account servicing payment service provider adds additional steps or required actions in the user journey compared to the equivalent authentication procedure offered to payment service users when directly accessing their payment accounts or initiating a payment with the account servicing payment service provider;	(~~j~~ i) imposing an account information or payment initiation journey, in a 'redirection' or 'decoupled' approach, where the authentication of the payment service user with the account servicing payment service provider adds additional steps or required actions in the user journey compared to the equivalent authentication procedure offered to payment service users when directly accessing their payment accounts or initiating a payment with the account servicing payment service provider;		
(k) imposing that the user be automatically redirected, at the stage of authentication, to the account servicing payment service provider's web page address when this is the sole method of carrying out the authentication of the payment services	~~(k) imposing that the user be automatically redirected, at the stage of authentication, to the account servicing payment service provider's web page address when this is the sole method of carrying out the~~		

PUBLIC

user that is supported by an account servicing payment service provider;	~~authentication of the payment services user that is supported by an account servicing payment service provider;~~		
(l) requiring two strong customer authentications in a payment initiation service-only journey where the payment initiation service provider transmits to the account servicing payment service provider all the information necessary to initiate the payment, namely one strong customer authentication for the yes/no confirmation and a second strong customer authentication for payment initiation.	(~~l~~ j) requiring two strong customer authentications in a payment initiation service-only journey where the payment initiation service provider transmits to the account servicing payment service provider all the information necessary to initiate the payment, namely one strong customer authentication for the yes/no confirmation and a second strong customer authentication for payment initiation.		
2. For the activities of payment initiation services and account information services the name and the account number of the account owner shall not constitute sensitive payment data.	~~2. For the activities of payment initiation services and account information services the name and the account number of the account owner shall not constitute sensitive payment data.~~		
Section 4			

PUBLIC

Rights and obligations of account information service providers and payment initiation service providers			
Article 45			
Use of the customer interface by account information service providers and payment initiation service providers			
1. Account information service providers and payment initiation service providers shall access payment account data exclusively via the dedicated interface referred to in Article 35, except in the circumstances covered by Article 38(4) and (5) and Article 39.	1. Account information service providers and payment initiation service providers shall access payment account data exclusively via the dedicated interface referred to in Article 35, except in the circumstances covered by ~~Article 38(4) and (5) and~~ Article 39.		
2. Where an account information service provider or a payment initiation service provider accesses payment account data via an interface that the account servicing payment service provider makes available to its payment service users for directly accessing their payment account, in accordance with Article 38(4) and (5), or where that is the only interface accessible in accordance with Article 39, the account	2. Where ~~an account information service provider or a payment initiation service provider accesses payment account data via an interface that the account servicing payment service provider makes available to its payment service users for directly accessing their payment account, in accordance with Article 38(4) and (5), or where that is~~ there is only the		

PUBLIC

information service provider or the payment initiation service provider shall at all times:	interface in accordance with Article 39 accessible ~~in accordance with Article 39,~~ to a payment initiation service provider or an ~~***the***~~ account information service provider, the account information service provider or the payment initiation service provider shall at all times:		
(a) identify itself towards the account servicing payment service provider;			
		(aa) provide information on the purpose of the access in accordance with article 43(2)(iii); *[**PRES comment**: Based on the comment of one MS suggesting that the ASPSP needs such information in order to fullfill obligation under article 43(2)(iii).]*	
(b) rely on the authentication procedures provided by the account servicing payment service provider to the payment service user;			
(c) take the necessary measures to ensure that they do not process data (including access and storage of data) for purposes other			

PUBLIC

than for the provision of the service as requested by the payment service user;			
(d) log the data that are accessed through the interface operated by the account servicing payment service provider for its payment service users, and provide, upon request and without undue delay, the log files to the competent authority. Logs shall be deleted 3 years after their creation. Logs may be kept for longer than this retention period if they are required for monitoring procedures that are already underway.			
For the purpose of point (d) logs shall be deleted 3 years after their creation. Logs may be kept for longer than this retention period if they are required for monitoring procedures that are already underway.	~~For the purpose of point (d) logs shall be deleted 3 years after their creation. Logs may be kept for longer than this retention period if they are required for monitoring procedures that are already underway.~~		
Article 46			
Specific obligations of payment initiation service providers			
1. Payment initiation service providers shall:			

PUBLIC

(a) provide account servicing payment service providers with the same information as the information requested from the payment service user when initiating the payment transaction directly;			
(b) provide services only where based on the payment service user's permission, in accordance with Article 49;			
(c) not hold at any time the payer's funds in connection with the provision of the payment initiation service;			
(d) ensure that the personalised security credentials of the payment services user are not, with the exception of the payer and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;			
(e) ensure that any other information about the payment services user obtained when providing payment initiation services, is only provided to the payee and only with the payment services user's permission;			
(f) every time a payment is initiated, identify itself towards the account servicing			

PUBLIC

payment service provider and communicate with the account servicing payment service provider, the payer and the payee in a secure way.			
2. Payment initiation service providers shall not:			
(a) store sensitive payment data of the payment service user;	(a) without prejudice to Article 45(2)(d), store sensitive payment data of the payment service user;		
(b) request from the payment service user any data other than those necessary to provide the payment initiation service;			
(c) process any personal or non-personal data (including use, access or storage of data) for purposes other than for the provision of the payment initiation service as permitted by the payment services user;			
(d) modify the amount, the payee or any other feature of the transaction.			
Article 47			
Specific obligations of and other provisions concerning account information service providers			

PUBLIC

1. The account information service provider shall:			
(a) provide services only where based on the payment service user's permission, in accordance with Article 49;			
(b) ensure that the personalised security credentials of the payment service user are not accessible to other parties, with the exception of the user and the issuer of the personalised security credentials, and that when those credentials are transmitted by the account information service provider, transmission is done through safe and efficient channels;			
(c) for each communication session, identify itself towards the account servicing payment service provider of the payment service user and securely communicate with the account servicing payment service provider and the payment service user;			
(d) access only information from designated payment accounts and associated payment transactions;			
(e) have in place suitable and effective mechanisms that prevent access to information other than from designated			

PUBLIC

payment accounts and associated payment transactions, in accordance with the payment service user's permission.			
2. The account information service provider shall not:			
(a) request sensitive payment data linked to the payment accounts;	(a) ~~request~~ access sensitive payment data linked to the payment accounts;		
(b) use, access or store any data for purposes other than for performing the account information service permitted by the payment service user, in accordance with Regulation (EU) 2016/679.	(b) ~~use, access or store~~ process any data for purposes other than for performing the account information service permitted by the payment service user~~, in accordance with Regulation (EU) 2016/679~~.		
3. The following Articles shall not apply to account information service providers: Articles 4 to 8, Articles 10, 11 and 12, Articles 14 to 19, Articles 21 to 29, Articles 50 and 51, Articles 53 to 79, and Articles 83 and 84.			
Section 5			
Implementation			
Article 48			
Role of competent authorities			

PUBLIC

1. Competent authorities shall ensure that account servicing payment service providers comply at all times with their obligations in relation to the dedicated interface referred to in Article 35(1) and that any identified prohibited obstacle listed in Article 44 is immediately removed by the relevant account servicing payment service provider. Where such non-compliance of the dedicated interfaces with this Regulation or obstacles are identified, including on the basis of information transmitted by payment initiation services and account information services providers, the competent authorities shall take without delay the necessary enforcement measures and impose any appropriate sanction or, where appropriate, grant access rights in accordance with Article 38(4).	1. Competent authorities shall ensure that account servicing payment service providers comply ~~at all times~~ with their obligations in relation to the dedicated interface referred to in Article 35(1) and Article 38(1), (2), (3), (4) and (5~~3~~) and that any identified prohibited obstacle listed in Article 44 is ~~immediately~~ removed as soon as possible by the relevant account servicing payment service provider. Where such noncompliance of the dedicated interfaces with this Regulation or obstacles are identified, including on the basis of information transmitted by payment initiation services and account information services providers, the competent authorities shall take without delay the necessary enforcement measures and impose any appropriate sanction ~~or, where appropriate, grant access rights in accordance with Article 38(4)~~.		
2. Competent authorities shall take without delay every necessary enforcement			

PUBLIC

action where necessary to preserve the access rights of payment initiation services and account information services providers. Enforcement actions may include appropriate sanctions.			
3. Competent authorities shall ensure that payment initiation service and account information service providers comply with their obligations in relation to the use of data access interfaces at all times.	3. Competent authorities shall ensure that payment initiation service and account information service providers comply with their obligations in relation to the use of data access interfaces ~~at all times~~.		
4. Competent authorities shall have the necessary resources, notably in terms of dedicated staff, in order to comply at all times with their tasks.	~~4. Competent authorities shall have the necessary resources, notably in terms of dedicated staff, in order to comply at all times with their tasks.~~		
5. Competent authorities shall cooperate with supervisory authorities under Regulation (EU) 2016/679 where processing of personal data is concerned.	4. Competent authorities shall cooperate with supervisory authorities under Regulation (EU) 2016/679 where processing of personal data is concerned.		
6. Competent authorities shall, on their initiative, hold regular joint meetings with account servicing payment service providers, payment initiation service and account information service providers and shall deploy their best efforts to ensure that	5 ~~6~~. Competent authorities shall, on their initiative and where necessary, hold ~~regular~~ joint meetings with account servicing payment service providers, payment initiation service and account information service		

PUBLIC

possible issues arising from the use of and access to data exchange interfaces between account servicing payment service providers, payment initiation service and account information service providers are rapidly et durably solved.	providers ~~and shall deploy their best efforts~~ to ensure that possible issues arising from the use of and access to data exchange interfaces between account servicing payment service providers, payment initiation service and account information service providers are ~~rapidly et durably~~ solved.		
7. Account servicing payment service providers shall provide competent authorities with data on access by account information service providers and payment initiation service providers to payment accounts which they service. Competent authorities may also, where appropriate, require account information service providers and payment initiation service providers to provide any relevant data on their operations. In accordance with its powers pursuant to Article 29, point (b), Article 31 and Article 35(2) of Regulation (EU) No 1093/2010, the EBA shall coordinate that monitoring activity by competent authorities, avoiding data reporting duplication. The EBA shall report every two years to the Commission on	6 ~~7~~. Account servicing payment service providers shall provide competent authorities with data on access by account information service providers and payment initiation service providers to payment accounts which they service. Competent authorities may also, where appropriate, require account information service providers and payment initiation service providers to provide any relevant data on their operations. In accordance with its powers pursuant to Article 29, point (b), Article 31 and Article 35(2) of Regulation (EU) No 1093/2010, the EBA shall coordinate		

PUBLIC

the size and operation of the markets for account information services and payment initiation services in the Union. Those periodical reports may, where appropriate, contain recommendations.	that monitoring activity by competent authorities, avoiding data reporting duplication. The EBA shall report every two years to the Commission on the size and operation of the markets for account information services and payment initiation services in the Union. Those periodical reports may, where appropriate, contain recommendations.		
8. The EBA shall develop draft regulatory technical standards specifying the data to be provided to competent authorities pursuant to paragraph 7 as well as the methodology and periodicity to be applied for such data provision.	7 ~~8~~. The EBA shall develop draft regulatory technical standards specifying the data to be provided to competent authorities pursuant to paragraph 7 as well as the methodology and periodicity to be applied for such data provision.		
The EBA shall submit those draft regulatory technical standards to the Commission by [OP please insert the date= 18 months after the date of entry into force of this Regulation].			
Power is delegated to the Commission to adopt the regulatory technical standards			

PUBLIC

referred to in the first subparagraph in accordance with Article 10 to 14 of Regulation (EU) No 1093/2010.			