Council of the European Union

Brussels, 17 April 2026
(OR. en)

8221/26

Interinstitutional File:
2023/0210 (COD)

LIMITE

EF 114
ECOFIN 477
CODEC 676
ECB

NOTE

From:	General Secretariat of the Council
To:	Permanent Representatives Committee
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulations (EU) No 1093/2010, (EU) No 260/2012, (EU) 2017/2394, (EU) 2021/1230 and (EU) 2023/1114 - Confirmation of the final compromise text with a view to agreement

2023/0210 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on payment services in the internal market and amending *Regulations* (EU) No 1093/2010, *(EU) No 260/2012, (EU) 2017/2394, (EU) 2021/1230 and (EU) 2023/1114*

(Text with EEA relevance)

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,

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 OJ C ▌, *C/2024/1594, 5.3.2024*.▌

2 OJ C ▌, *C/2024/3869, 19.6.2024*.▌

(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 ***have*** 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 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).

[4] COM/2020/592 final.

(3) Directive (EU) 2015/2366 aimed ***to address*** barriers to new types of payment services and ***to improve*** 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 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 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 ***the margin for*** 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 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 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.

---

[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).

(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 ***are not allowed to*** 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 local authorities when not acting in their capacity as public authorities.

▌

(9) The exclusion from the scope of Directive (EU) 2015/2366 of certain categories of operators of automated teller machines (ATM) has proven difficult to apply in practice. Therefore, the category of ATM ***deployers*** 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 ***deployers*** which do not service payment accounts. ▌Those ***deployers, which are*** subject to ***registration*** under Directive (EU) XXX [PSD3], ▌should▌ be subject to requirements on fees transparency in situations where such ATM ***deployers*** levy charges for cash withdrawals.

---

[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).

(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 provided by retailers on a voluntary basis and should depend on the availability of cash ***at*** 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 ***from*** 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 ▌ . 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 ***should be*** achieved by requiring that agents ▌ 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 ***scope*** 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.

(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 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.

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

(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 ***or*** online ▌ 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 instruments to meet the objectives laid down in social legislation, such as childcare vouchers or ecological vouchers. ***At the same time, the Member States' regulatory environment for vouchers should ensure the acceptability of such 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.

(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 ▌ 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. ***That exclusion*** should apply only where the value of payment transactions is below a specified threshold. ***For the exclusion to apply, the telecommunications operator must provide the payment services in addition to the electronic communications services it provides to its subscriber. That implies that there is a direct contractual arrangement between the telecommunications operator and the subscriber for the provision of the electronic communications services and that the payment service 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, they 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 factories', allowing for the centralisation of payment transactions of the same group. In that respect, payment transactions ***and related services*** 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***, including the redistribution through intragroup payment transactions of funds received from external third parties on behalf of group entities as well as the collection of payment orders and payment funds on behalf of a group by a parent undertaking or its subsidiary for onward transmission and processing to a payment service provider providing payment services to the group***. ▌ ***Insofar as public service operators within the meaning of Regulation (EC) No 1370/2007 handle equalisation payments and revenue sharing within a closed payment processing system of transport operators or via their clearing centres, tariff organisations or associations, those payment transactions should as well be excluded from the scope of this Regulation. Those exclusions should not be used to circumvent or evade Union or national law in the field of anti-money laundering and combating the financing of terrorism or the rules on authorisation and supervision of payment institutions.***

(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 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.

(17) Technical services do not constitute payment services ***in so far*** 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***, which should be limited to direct financial damage and should not exceed the amount of the transaction concerned***, or the requirement to enter into outsourcing agreements with payment service providers in case technical service providers are to provide and verify 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.

▌

(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 feature of the concept of payment account. ▌ A payment account should therefore be defined as an account that ***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 or where the account is used only for the execution of one transaction, 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*** used for sending and receiving funds to or from a third party ***are*** therefore ***excluded*** from the definition of a payment account.

(21) Given the emergence of new types of payment ***instruments, the evolving technological solutions providing such*** 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 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 ***either*** the tokenisation of an existing payment instrument, for example a payment card***, or a credit transfer from a payment account***, are to be considered as technical services and should thus be excluded from the ***definitions*** of payment instrument ***and of payment initiation service, provided that no funds are stored*** in the ***digital wallet, that the digital wallet provider never enters into possession of such funds and that the wallet provider operates under contractual arrangements within a closed system with the payment service providers servicing the payer's payment account or issuing the payer's payment instrument.*** 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-funded*** electronic wallets such as 'staged-wallets'***, characterised by a funding-stage and a payment-stage***, should be considered a payment instrument and their issuance a payment service. ***This includes both wallets where users store funds in advance for future transactions and wallets where the funding stage and the payment stage occur simultaneously at the time of the transaction, including where the wallet is automatically funded, in whole or in part, from a linked payment instrument or account.***

[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).

(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 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 ***consent*** 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. ▌ 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 ▌ to receive other - non-payment - services including lending, accounting, creditworthiness assessment. It is however essential that payment service users know 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 ***consent***. 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.

▌

(28) The definition of funds should cover ▌ central bank money issued for retail use, including banknotes and coins, and any possible future central bank digital currency, e-money***,*** ***including electronic money tokens,*** 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***, as defined in that Regulation, are*** deemed to be electronic money. ***That is regardless of whether the*** electronic money tokens ***meet the definition of electronic money in [PSD3] and this Regulation. Accordingly, references to electronic money in this Regulation should be understood to include electronic money tokens, unless otherwise stated in this Regulation, and electronic money tokens should be*** included, as electronic money, in the definition of funds***. Likewise, providing transfer services for crypto assets on behalf of clients as defined in Regulation 2023/1114 with electronic money tokens could qualify as the payment service of execution of payment transactions, including when such transfers are provided as part of other crypto-asset services, unless such transfers are covered by a specific exclusion from the scope of*** this Regulation ***and Directive xx [PSD3]***.

(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 activities. This concerns in particular the exchange by crypto-asset service providers of electronic money tokens for funds or crypto-assets, where the crypto-asset service providers is acting in its own name as buyer or seller of those electronic money tokens, as well as the exchange of electronic money tokens for electronic money tokens or crypto-assets carried out by a crypto-asset service provider intermediating between buyers and sellers. 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 provided by a CASP where electronic money tokens are used to pay for goods or services.

(29b) Taking into account that 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 also include a similar exclusion as regards 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.

(30) To preserve the confidence of the electronic money holder, electronic money needs to be redeemabl. 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 action targeting the freezing of funds or any specific measure linked to the prevention and investigation of crimes.

---

[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).

(31) Payment service providers need access to payment systems ***and to payment schemes*** to provide payment services to users. Those payment systems typically include ▌ major systems processing credit transfers and direct debits***, whereas payment schemes typically include four-party card schemes***. 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 ***and schemes***. Such access may be direct or indirect via another participant in that payment system ***or scheme***. Such access should be subject to requirements that ensure integrity and stability of those payment systems ***and schemes***. To that end the payment system operator ***or the payment scheme operator, as the case may be,*** 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 participation in a payment system ***or scheme*** should bear the risk of its own choice of system ***or scheme*** and provide proof to the payment system ***or scheme*** that its internal arrangements are sufficiently robust against those types of risk. Payment system ***operators and payment schemes*** 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 ***scheme or*** poses an unacceptably high level of risk.

(31a) Payment service providers and technical service providers that provide services to payment service providers should be able to secure interoperability with, and to have access for the purposes of interoperability to hardware and software features provided or controlled by original equipment manufacturers of mobile devices or electronic communications service providers, that are necessary to process and execute payment transactions online or offline in a competitive way. Those technical features include hardware and software that is necessary to manage the transaction flow between the payment method and the acceptance device, such as near filed communication technology (NFC) on mobile devices and the payment terminal kernel, or to ensure that mobile payment applications run in a secure environment that protects cryptographic keys and algorithms, the customer PIN code or biometric data, such as the so-called secure elements of mobile devices (e.g.: Universal Integrated Circuit Card (UICC), embedded SE (eSE), and microSD etc). Original equipment manufacturers of mobile devices and electronic communications service providers should be obliged to enable interoperability with, and provide access to all hardware and software features that are necessary to process and execute online and offline transactions on fair, reasonable and non-discriminatory terms. That obligation should be without prejudice to Article 6(7) of Regulation (EU) 2022/1925 of the European Parliament and of the Council1, which obliges gatekeepers to provide, free of charge, effective interoperability with, and access for the purposes of interoperability to, the operating system, hardware or software features of mobile devices and which is applicable to existing and new digital means of payments.

(32) Payment system operators ***and operators of payment schemes*** should have in place rules and procedures on access which are proportionate**,** objective**,** non-discriminatory and transparent. Payment system operators ***and operators of payment schemes*** should not discriminate against payment institutions as regards participation if the system ***or scheme*** rules can be respected and there is no unacceptable risk to the system ***or scheme***. 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 oversight by the European System of Central Banks under Regulation ***(EU) No 2025/1355***, the central bank or banks exercising that oversight should monitor ***the*** respect of those rules in the framework of their oversight. In cases of other payment systems ***or schemes***, Member States should designate national competent authorities to ensure that payment system infrastructure operators ***and operators of payment schemes*** respect such requirements***, if those requirements are not enforced under the oversight of the operations of those other payment systems or schemes by the Eurosystem or central banks of non euro area Member States***.

---

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).

(32a) Higher costs for payment service providers providing acquiring services of card-based payment transactions and merchants result from the lack of transparency of pricing applied by operators of payment card schemes and processing entities - for instance because acquirers and merchants are not aware of the actions to take to avoid behavioural fees, or which service is optional, or how to opt out of an optional service. This ultimately harms consumers due to the pass-through by merchants of their increased card-acceptance costs, resulting in higher retail prices. Since consumers are likely to decrease their consumption as a result, merchants' turnover is negatively impacted, unless merchants absorb these costs, thereby decreasing their profit margin. Scheme fees and processing fees should therefore be transparent, but also able to be compared, to allow providers of acquiring services to maximise the efficiency of scheme and processing services they source and supply, creating the conditions for efficiency gains to trickle down to merchants, via lower merchant service charges for the acceptance of card-based payments, and to consumers, via lower retail prices. At the same time, providers of acquiring services and merchants can only make truly informed choices of scheme and processing service if they are promptly informed about any new scheme and processing fees or any change to fees. Regulation (EU) 2015/751 on interchange fees for card-based payment transactions lays down transparency requirements that acquirers are subject to vis-à-vis payees they contract with. Acquirers should ensure that the level of transparency of the information that they are provided with regarding scheme and processing services and the corresponding fees is shared with merchants, when fulfilling their obligations under Regulation (EU) 2015/751. Due to the complex nature of the payment card schemes' and processing entities' billing system, and for the transparency requirements to be effective and proportionate, 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 further specify the information to be disclosed to payment service providers providing acquiring services regarding scheme and processing services and the corresponding fees.

(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 ***and schemes*** should not apply to systems ***and schemes*** set up and operated by a single payment service provider. Such payment systems ***and schemes*** can operate either in direct competition to other payment systems ***or schemes*** or, more typically, in a market niche not covered by other payment systems ***or schemes. Such schemes*** 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 ***system*** 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 ***and schemes*** to established mainstream payment systems ***and schemes***, access to those closed proprietary payment systems ***and schemes*** should not be granted to third parties. However, such closed systems ***and schemes*** should always be subject to Union and national competition rules which may require that access be granted to the ***systems or*** schemes in order to maintain effective competition in payments markets.

(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 ***payment service users'*** funds***. Payment institutions should also endeavour not to safeguard all payment service users' funds with one credit institution in order to avoid, where appropriate, concentration risk***. However, as evidenced in particular by the EBA in its Opinion of 5 January 2022,[12] 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.

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

(36) Credit institutions should therefore provide***, on an objective, non-discriminatory and proportionate basis, access to*** a payment account to payment institutions, and to applicants for a license as a payment institution, as well as to their agents ▌. It is necessary to include applicants for a ***authorisation*** as a payment institution in that provision, given ***that an*** account ***with a credit institution*** where clients' funds can be safeguarded is a prerequisite to obtain a payment institution ***authorisation. Credit institutions*** should ***be able to refuse access to payment accounts only in exceptional cases where there are*** serious grounds ***to do so. Credit institutions should be able to refuse to open or be able to close a payment account for a*** payment institution, ***its agents or an applicant for an authorisation as a payment*** institution ▌ where ***this would result in an infringement of Regulation (EU) 2024/1624 of the European Parliament and of the Council. Credit*** institutions ***should also be able to refuse such access in cases where relevant information or documents have not been received from the applicant to open an account as this may impede, inter alia, their ability to perform customer due diligence obligations. A payment institution or its*** agents ***or an applicant for authorisation as*** 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 ***give reasons*** in writing and in detail ***for*** any refusal to provide an account, or a subsequent closure of an account. ***Those reasons*** 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 opening or maintaining such an account would result in infringement of Regulation (EU) 2024/1624 of the European Parliament and of the Council, the justification provided to the client or the applicant should not lead to the disclosure of information protected under Article 73 of that Regulation.*** To facilitate treatment by competent authorities of appeals against account refusal or withdrawal and ***reasons*** thereof, the EBA should develop implementing technical standards harmonising the presentation of such ***reasons***.

(37) To make well-informed choices and to be able to choose their payment service provider easily within the Union, payment service users should receive comparable ▌ information about payment services ***in a clear, neutral*** and comprehensible ***manner. To ensure that such*** 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.

(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 ***at those users'*** request. In the second situation, payment service users ***need to*** 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. 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. ***Such agreements with undertakings and organisations who are not consumers could govern whether or not strong customer authentication (SCA) is applied.*** Micro-enterprises, as defined in Commission Recommendation 2003/361/EC,[13] ***could*** be treated in the same way as consumers. Certain rules should always apply, irrespective of the status of the user.

(39a) Payment service providers, including ATM deployers, should display to their customers in a clear, neutral, and comprehensible manner, information on any charges both before the customer initiates the withdrawal and while carrying 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 paper or another durable medium.

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

(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 ***or on another durable medium***, 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 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 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 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 paper or on another durable medium,*** on all applicable charges for domestic ATM withdrawals in different situations, depending on the ATM from which the payment service users withdraw cash. ***For ATM withdrawals denominated in euro, any charges payable by payment service users to their payment service provider, including where withdrawals are made at ATMs operated by independent ATM deployers, should be subject to the principle of equality of charges, as set out in Article 3 of Regulation (EU) 2021/1230. That Regulation should be amended accordingly.***

(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 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.

(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 ***3*** 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 ***not*** be longer than 1 month, and for payment service providers***, not*** shorter than ***3*** 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 ***monetary amount in the currency of the payer's account and as a*** percentage mark-up over ***an aggregated mid-market*** exchange ***rate that accurately reflects the market. To ensure that the exchange 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. A payment service provider should use the same*** reference ***benchmark consistently and for exchanges made in both directions***. When reference is made to 'charges' in this Regulation, it should also cover, where applicable, 'currency conversion' charges.

(50a) The payment service provider of the payer should provide an estimate of 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. 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) Since a payment service provider can provide or make available the name of the payee to the payer only where such information is available to it, this requirement cannot be applied in circumstances where it is not feasible to do so. This is generally the case for money remittances executed as a single payment transaction, where the payer's payment service provider does not have access to the name of the payee unless it is provided by the payer. It is therefore appropriate that, in such cases, the payer's payment service provider is not required to provide or make available the payee's name 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 ***might*** also be zero as the rules should not affect the practice whereby a payment service provider does not ***levy any charges on the payer or the payee***. Similarly, ***without prejudice to Union competition rules and to Regulation [IFR] and*** depending on the contract terms, ***the*** payment service provider ***of the payee might*** charge only the payee for the use of the payment service ***where such charge includes a compensation to the payment service provider of the payer and the payer's payment service provider is not imposing*** charges ▌ on the payer. It is possible that ▌ 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 ***or compensation*** between payment service providers or any intermediaries.

(52) A surcharge is a charge by merchants to consumers that is added ***to*** 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 European Parliament and of the Council[14] 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.

[14] 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).

(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 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 ***payment account*** 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 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 could also transmit the payment account data obtained to a third party who in turn would provide a service to the payment service user leveraging on that data, possibly with additional value added services.*** Payment initiation services allow the initiation of a payment from the user's account, such as a credit transfer ▌, 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 Regulation (EU) 2024/1624, 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 not only to the payer, but in certain cases, also to the payee. The provision of a pass-through digital wallet enabling the user to initiate a payment from the user's payment account, provided that no funds are stored in the digital wallet, that the digital wallet provider never enters into possession of such funds and that the wallet provider operates under contractual arrangements with the payment service providers servicing the payer's account, should not be considered a payment initiation service.***

(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 ***consent*** 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 payment markets, could be very significant. That principle should therefore be maintained. Maintaining that approach is in line with Chapters III and IV of ▌ Regulation ***(EU) 2023/2854*** on harmonised rules on fair access to and use of data (Data Act)[15], in particular Article 9(3) of that proposal on compensation, to which this Regulation is without prejudice. ▌

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

(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 ***Regulation (EU) 2023/2854*** 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 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 ▌ 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 ***be able to choose which authentication method they offer to the payment service user, in order to offer the least burdensome option. Account information and payment initiation service providers should*** use the interface dedicated for their access **.** In cases of failure or ***unplanned*** unavailability of the dedicated interface ▌ their business continuity would be endangered by their incapacity to access the data for which they have been granted ***consent***. It is ***essential*** 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, 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 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.***

(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 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) ***or other widely recognised standards offering an equivalent level of security, which would allow account servicing payment service providers to benefit from a wide range of technological solutions without compromising security or relying on niche standards that would be difficult for third-party providers to implement***.

(59) ***In order*** 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 clients, the dedicated interface that they are ***required*** to use ***should enable a straightforward and seamless user experience by meeting*** 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 ▌. More detailed requirements for dedicated interfaces should be laid down in Regulatory Technical Standards developed by the EBA.

(59a) For the purpose of effective verification prior to payment initiation, account servicing payment service providers should ensure that payment initiation service providers can verify the full name of the account holder via the dedicated interface, and should therefore not provide partial or abbreviated names.

(60) Given the dramatic impact that a prolonged ***unplanned*** unavailability of a dedicated ▌ interface would have on account information and payment initiation service ▌ providers' business continuity, account servicing payment service providers should ***use their best efforts to prevent any unplanned unavailability or underperformance of that interface. Underperformance should be understood as performance falling below that of the interface used by the account servicing payment service provider for authentication and communication with its payment service users. Account servicing payment service providers should*** remedy ***any*** such unavailability ***or underperformance*** without ***undue*** delay ***and ensure an optimal recovery time for 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*** should be ***mandated to clarify, in the draft regulatory technical standards, the requirements related to the quarterly statistics on the availability and performance of dedicated interfaces 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. That severity should take into account, among others, the number of customers impacted and types of functionality of account information and payment initiation service providers affected.***

(61) ▌ Account information and payment initiation service providers should ▌ always duly identify themselves and respect all their obligations, such as the limits of the ***consent*** 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 ***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 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, meaning a specific, secure digital connection point that allows automated, machine-to-machine communication and data exchange,*** or not to offer any open banking data access interface at all***. Where appropriate, according to the specificities of the Member State, for national central banks not acting in their capacity as monetary authority or other public authorities, the exemption from the obligation to have in place a dedicated interface may be granted by the Member State***. Data access via the customer interface (with no dedicated interface) may be appropriate ***where that interface is already an API, such as in B2B cases where no mobile applications or website interfaces are used between*** the ▌ account servicing payment service provider ***and its customer, or where*** a dedicated interface would be a significant financial and resource burden ***for the account servicing payment service provider, such as for very small payment service providers***. 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 ***be of*** no relevance to its customers. Detailed criteria for granting such ▌ exemption 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***. ***Such exemptions, once granted, should not be perpetuated if the circumstances which led to the exemption changes significantly.***

(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 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***, and on an ongoing basis, at the request of a payment initiation service provider***. 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 ***have access to*** the information necessary to assess the risks of non-execution of the initiated transaction. That information is indispensable to enable the payment 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 ***consents*** that those payment service users have granted to payment service providers, including the purpose of ***the consent*** and the categories of payment account data concerned, ***such as*** 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. ***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.***

Consent for initiation of one-off payments should not feature on that dashboard. A dashboard ***should*** not allow a payment service user to establish new data access ***consents*** with an account information or payment initiation service provider to which no previous data access has been given. Account servicing payment service providers should ***promptly make information available to*** account information and payment initiation service providers ▌ 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 ***consents*** granted by payment service users, including the duration of validity of the ***consent*** 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 ***consents*** 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 ***consent*** dashboard should empower customers to manage their ***consents*** 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 ***consent*** 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 purpose of providing the account information service, where the payment service user does not actively request such information, but the payment service user has given their consent. In that case, the payment service user must be informed by the account information service provider, but that information obligation does not have to be fulfilled on an access by access basis, but may be fulfilled by including that information in the 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 ▌ the prohibition on such obstacles imposed by Article 32(3) of Commission Delegated Regulation (EU) 2018/389[16]. 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 ***Opinion of 4*** June 2020 ***on*** obstacles ▌ under ***Article 32(3) of the RTS on SCA and CSC[1]***. Despite clarifications efforts made***,*** there is still a lot of uncertainty, in the market and with supervisors, as to what 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.

---

16 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).

(66a) The possibility to rely on fraud prevention or compliance with Regulation (EU) 2016/679 should not serve as a general basis to deny, restrict or delay data access by third party providers. Measures taken on those grounds could exceptionally restrict access to open banking services but should be allowed on a case-by-case basis only where duly justified, based on objective and verifiable elements of suspected fraud or on a specific GDPR obligation, and should remain strictly necessary, proportionate and limited in scope and duration. They should not lead to systematic or blanket restrictions to open banking, nor legitimize obstacles to data access which are prohibited under the current Regulation. While account servicing payment service providers may legitimately take measures to mitigate fraud, such measures should not discriminate against the services provided by providers of payment information and account information services. As such, they should be equally applied to such services, as to payment services provided directly or indirectly by the account servicing payment service provider itself, including card- or credit based payment services which are commercially available for payees to use. That principle should apply to both the payer authentication experience and to the rate of certainty that an initiated payment is executed by the account servicing payment service provider.

(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 ***provision*** 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 (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 ***unique identifier*** 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 ***enforcers*** of open banking ▌ . It is essential that national competent authorities ***deploy their best efforts to*** ensure the respect of the Union 'open banking' regulated framework ▌ . National competent authorities should have the appropriate resources to perform their enforcement tasks effectively and efficiently. National competent authorities should ***facilitate*** a smooth and regular dialogue between the various actors of the 'open banking' ecosystem***. In particular, it must be ensured that account servicing payment service providers comply at all times with their obligations in relation to the dedicated interface***. Account servicing payment service providers and account information and payment initiation service providers which do not comply with their obligations should be ***subject*** to appropriate sanctions. Regular monitoring of the 'open banking' market in the Union by ***national*** competent authorities, coordinated by the EBA, should facilitate enforcement, and collection of data on the 'open banking' market ***should*** 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 ▌ Regulation ***(EU) 2023/2854 on harmonised rules on fair access to and use of data (Data Act)***.

(68a) The dedicated interface should be the primary access point for AIS and PIS. Besides, some ASPSPs might have additional interfaces for other application contexts, which are technically able to provide the same services for AISPs and PISPs as the dedicated interface. AISPs and PISPs should be able to use those additional interfaces with the permission of the ASPSP. However, that possibility must not be interpreted as an obligation for the ASPSP to grant access through anything else than the dedicated interface, nor does it stipulate any right for AISPs and PISPs (or other unregulated entities) to demand such access. The additional interfaces can only be used if the participants want to do so on their own accord, with agreement by ASPSPs and under the same security conditions (identification and secure communication) that also apply for the dedicated interface and if the additional interfaces use widely accepted and interoperable standards.

(69) 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 that legal basis laid out in that*** Regulation ***are met.***

(69b) A payment transaction or a series of payment transactions should be considered as authorised only if the payer has given its consent for the execution of the payment transaction in a manner agreed on between the payer and the account servicing payment service provider. It should not be considered to be authorised where the transaction was initiated or modified by a third party who is acting without the consent of the payment service user. Instances of payment transactions initiated or modified by a third party acting without the consent of the payment service user include situations where that third party is using the payment service user's personal security credentials fraudulently obtained.

(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 which ***verifies*** whether ▌ the unique identifier of the payee and the name of the payee***, as*** provided by the payer***, match*** and, should ***a mismatch*** be detected, ***notifies*** the payer thereof***. Where the payee is a legal person, this service could be carried out by verifying a match between the unique identifier of the payee and another data element, such as a fiscal number, a European unique identifier as referred to in Article 16(1), second subparagraph, of Directive (EU) 2017/1132 of the European Parliament and of the Council***[7]***, or a legal entity identifier (LEI), that unambiguously identifies the payee, if the payer is allowed to submit such data element via a payment initiation channel of the payer's payment service provider and such data element is available in the internal systems of payee's payment service provider. Where the payment account of the payee is not identified by IBAN, other type of unique identifier should be used to unambiguously identify the payment account of the payee***. 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 ***payment service users***. 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 ***both*** the unique identifier and the name of the payee***. In such cases, the payment service provider should ensure that the payee to whom the payer intends to send a credit transfer is identified correctly***.

---

[7] ***Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification) (OJ L 169, 30.6.2017, p. 46***

(71) Regulation (EU) ***2024/886*** amending Regulation (EU) No 260/2012 provides for a service verifying the match between the unique identifier and the name of the payee ***or another data element*** to be offered to users of ***credit transfers in euro, including*** 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) ***2024/886*** amending Regulation (EU) No 260/2012 ***and should be aligned with the verification service provided for by Regulation (EU) 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 identification documents in case of natural persons, or differences between commercial and legal names in case of legal persons. To avoid undue frictions in ***situations where the name of the payee provided by the payer and the name associated with the IBAN or, where IBAN is not used to identify the payment account, another type of unique identifier, which was provided by the payer, do not match exactly but nevertheless almost match and to*** facilitate the payer's decision on whether to proceed with the intended transaction, payment service providers should indicate ***to the payer the name of the payee associated with the IBAN or another type of unique identifier provided by the payer*** in the ***manner which ensures compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council***.

(73) Authorising a payment transaction despite the matching verification service having detected a ***mismatch*** and notified that ***mismatch*** 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 ***mismatch*** and proceed with the execution of the transaction. Payment service users ***that are not consumers*** should be able to opt out from ***receiving the*** service ***ensuring verification of payee when submitting payment orders via payment initiation channels that are based on automated dedicated processes or protocols and that are only made available to*** payment service ***users that are not consumers***. After opting out, ***such*** payment service users should be able to avail again of the service. ***Moreover, in order to allow for a more smooth integration of the service ensuring verification in payment management processes of such payment service users, payment service providers should offer them the possibility of agreeing in the framework contract that the service ensuring verification with respect to payment orders placed via such payment initiation channels is provided after authorisation of those orders and that, in case of certain specific outcomes of the service ensuring verification, the payer's payment service provider executes those orders without any further input from the payment service user. Regulation 260/2012 should be amended accordingly.***

(73b) In order to allow the payment service user to protect itself, the payment service provider should offer the payment service user the possibility to set, in the framework contract, a limit of a maximum amount that can be transferred via a payment method or a payment instrument. Furthermore, it should be possible for the payment service user to set limits which differ for each means of payment and each payment instrument and which are expressed, at the sole discretion of the payment service user, on a transaction basis or within a set timeframe, such as a day or a week. Where the payment service provider proposes a limit for credit transfers to be set by the payment service user, the proposed limit should be the same for different types of credit transfers, so that the payment services user is not unknowingly prevented from having the same access to instant credit transfers as to other types of credit transfers. Payment services users should also be able to modify limits that have been previously set in the framework contract.

(73c) To ensure the effectiveness of the spending limits, it is important that any increase in the limits that is requested by the payment service user through a remote channel take effect only after a delay period. If such a delay period is not in place a fraudster could convince a victim to adjust the victims' spending limits and then immediately be able to defraud a victim of a much higher value. A delay period would give the payment service user time to realise that they have been contacted and manipulated by a fraudster. The delay period should by default be set at 4 hours by the payment service provider. The payment service user should be able to adjust the delay period upwards or downwards or opt out of the application of such a delay period with such actions being subject to the delay period in place. The application of strong customer authentication should be required when the payment service user requests an increase in spending limit through a remote channel.

(73d) The payment service provider's decision to block the payment instrument should be based on objectively justified reasons based on the data acquired through the transaction monitoring mechanism, and should 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 of objectively justified reasons might include suspicion of unauthorised use, suspicion of fraudulent transactions, security of payment instrument, risk of deception regarding financial activity and transactions carried out at long distances from each other in an unjustifiably short timeframe.

(73e) ***As payment services become increasingly digital, many payment service providers are offering payment service users the possibility of using mobile applications to initiate payment services. While these mobile applications are useful and beneficial to payment service users, they also pose a fraud risk. To prevent this risk, the process of activating a mobile application on a device should require the use of different communication channels, where there is an existing customer relationship between the payment service user and the payment service provider, and the application of strong customer authentication. When establishing the customer relationship, the payment service provider and the payment service user should agree on a delay for the activation of a subsequent mobile application to take effect in order to allow the payment service user to intervene if they are not the one activating the mobile application. To allow for a convenient process of establishing a customer relationship, also known as onboarding, this delay period should specifically not apply when the mobile application is used to establish the customer relationship between the payment service user and the payment service provider. The payment service provider should set a delay period of 4 hours. The payment service user should afterwards have the right to adjust or opt out of the application of such a delay period, in which case the application of strong customer authentication should be required. Any adjustment of the timeframe of the delay period requested by the payment service user should itself be subject to the delay period proposed by the payment service provider, and could be upwards or downwards from the period of 4 hours. The payment service provider should also notify the payment service user in a secure manner, and through different communication channels, of the activation of a mobile application linked to their payment account on a device if there is an existing customer relationship between the payment service provider and the payment service user. The purpose of the notification is to increase the vigilance of the payment service user and should enable the payment service user to alert the payment service provider if they have not installed the mobile application themselves. In that case, the payment service provider should ensure that the mobile application does not allow access to the payment account of the payment service user or the initiation of payment transactions. This should not apply to the activation of a mobile application on a device of the payment service user, if done by the payment service provider at its physical premises, and it should not apply to the initial establishment of the customer relationship between the payment service provider and the payment service user because no funds nor a payment account of the payment service user are available through the***

payment service provider at the point of establishing the customer relationship and because it would not be possible for the payment service provider to contact the specific payment service user, given that, at the point of onboarding, the payment service provider has not yet verified contact information for the payment service user.

(73f) Payment service providers should ensure, in their communications with their customers, that any information which, if unduly intercepted, might result in the compromise of the security of the payment instrument or security payment credentials is transmitted to the customer through safe and efficient communication channels.

(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 ***for*** a refund to their account servicing payment 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.

(76a) 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 should not in itself necessarily be considered sufficient to prove that the payment transaction was authorised by the payer. The authentication or the use of the strong customer authentication recorded by the payment service provider, including the payment initiation service provider, as appropriate, should not alone necessarily constitute sufficient evidence 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.

(76b) In order for the payment service user to have an easier access to the payment service provider, the latter should create and serve a communication channel to enable the payment service user to make a notification or to request unblocking of the payment instrument as provided for in this Regulation. That channel should also make it possible for the payment service user to make a notification about a fraudulent transaction. Payment service providers could use the channel to provide advice to a customer that suspects they are a victim of a fraud attack and for payment service users to notify problematic issues concerning conducted payments, such as errors of relevant devices during execution of the payments.

(76c) Given the increasing complexity and rapidly changing patterns of fraud, it is appropriate to ensure that, before a payment service provider concludes that a payment service user acted fraudulently or with intent or gross negligence and therefore refuses a refund to that payment service user in accordance with this Regulation, that payment service user should be given the possibility to provide to their payment service provider, in support of their claim, any relevant information or evidence concerning the circumstances of the disputed payment transaction or series of payment transactions. In that context, where a payment service user denies having authorised one or a series of payment transactions, or where a payment service user who is a consumer claims that one or a series of payment transactions were the result of fraud involving the impersonation of the payment service provider within the meaning of this Regulation, the payment service provider should not conclude that that payment service user, or consumer, as applicable, acted fraudulently or with intent or gross negligence, without previously having invited proactively and unambiguously that payment service user to provide any such information or evidence, and without having duly considered it in its assessment. The obligation of the payment service provider to enable the payment service user to supply relevant evidence or information in support of their claims should be construed as a right of the payment service user to have all relevant information concerning the circumstances of the disputed payment transaction or series of payment transactions duly assessed by the payment service provider. That should not be construed as a ground for the payment service provider to conclude that the payment service user acted fraudulently or with intent or gross negligence where the payment service user does not provide evidence that they cannot reasonably be expected to have such as, for example, voice call recordings, or where the payment service user does not provide any evidence or information.

(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 ***the payment service provider suspects that such*** unauthorised transaction ***resulted from the payer failing with intent or gross negligence to fulfil one or more of their obligations with regard to the security of payment instruments and personal security credentials, or*** from fraudulent behaviour by the payer***,*** and where that suspicion is based on ***objectively justified reasons***, the payment service provider should be able to conduct an investigation before refunding the payer. The payment service provider should, within ***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. ***Where the payment service provider refuses the refund after concluding from its investigation that the payer acted fraudulently, the payment service provider should communicate the reasons for that conclusion to the relevant national authority. Member States should provide clear public indication as to the relevant national authority to which such communication by the payment service provider is to be addressed.*** 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***, loss or misappropriation*** of a payment instrument ***or personalised security credentials,*** 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, ***at the date of adoption of this Regulation*** an amount of EUR 50 ***is*** 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 ***or personalised security credentials***. Moreover, once a payment service user has notified a payment service provider that his or her payment instrument ***or personalised security credentials*** may have been compromised, the payment service user should not be required to cover any further losses stemming from unauthorised use of that ***payment*** instrument ***or personalised security credentials***. 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 ***provision*** or malfunctioning of the service ***verifying the match*** between the name and unique identifier of a payee would create the right incentives for payment service providers to provide a fully functioning service, with the aim of reducing the risk of ill-informed payment authorisations. ▌ The payment service provider of the payer should be held liable ***and without delay should refund the payer*** the full amount of the ***defective*** credit transfer ***which results from a failure of*** that payment service provider ***to provide, or to provide correctly,*** the payer ***with the service of*** payee ***verification***. Where the liability of the payment service provider of the payer is attributable to the payment service provider of the payee ***or to the payment initiation service provider***, the payment service provider of the payee ***or, where relevant, the payment initiation service provider*** should compensate the payment service provider of the payer for the financial damage incurred.

(78a) Payment service providers should cooperate with payment service users and with competent authorities in cases where the correct provision of the verification of payee service is questioned.

(79) ***Payment service users*** should be adequately protected in the context of ***so-called social engineering fraud, where a fraudster manipulates a*** payment ***service user in performing a certain action, such as initiating a payment transaction, or handing over the payment service user's security credentials to the fraudsters***. The number ***of such type*** of 'social engineering' cases ▌ has significantly increased in recent years. ▌ Those new types of ▌ 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 ***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 ***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 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. ***It is therefore necessary to define the conditions under which a payment service user has a right to a refund.***

(80) ***Fraudsters often rely on tools and techniques such as caller ID, electronic mail address, or IP address*** ‘spoofing’***. Such fraud*** cases ***are complex, often involving different actors along the fraud scheme chain.*** Payment service providers have more means than consumers to put an end to these fraud cases***. Both payment service providers and electronic communications services providers can play a critical role in preventing fraud*** through adequate prevention and robust technical ***measures. Payment service*** providers ***are subject to specific obligations under Regulation (EU) 2022/2554 on digital operational resilience for the*** financial ***sector which aims at mitigating ICT risks. Regulation (EU) 2022/2554 subjects payment service providers to a comprehensive set of rules on ICT risk management framework, including tools, policies and procedures to protect the confidentiality, integrity and availability of data whether at rest, in use or in transit. For the purpose of complying with those obligations, payment service providers should have in place adequate technical measures and tools to prevent the fraudulent replication and misuse of the payment service provider’s domain name and of the communication channels used for communication between the*** payment service provider and ***the payment service user, including*** the payment service provider***’s electronic*** mail address ***and calling line identification***. ▌

(80a) ***Cases of payment service provider impersonation (spoofing) fraud affect the good reputation of the payment service provider, and of the financial sector as a whole and may cause significant financial damages to Union consumers, affecting their trust in electronic payments and in the financial system. A consumer who has been the victim of such cases of 'spoofing' fraud, where fraudsters pretend to be the consumer's payment service provider and misuse the domain name or the communication channels attributed to the consumer's payment service provider, for example, the payment service provider's e-mail address, telephone number, website or mobile application, 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'. Where the fraud concerns the payment service provider's website or mobile application, the refund right should encompass both cases involving the appropriation of those channels by the fraudster and fraudulently created versions of the website or mobile application that mirror the contents of the real ones. As soon as the 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 his or her payment service provider, and to the police, preferably via online complaint procedures, where made available by the police. Given that especially vulnerable consumers might have difficulties in reporting the fraud to the police in a timely manner, payment service providers are encouraged to assist the consumer in such reporting, where necessary.***

(80b) Payment fraud including the initiation or modification of payment orders without the payer's consent, the theft of sensitive payment data, including personal security credentials, or the manipulation of the payer, including by means of impersonation, frequently involves fraudulent activity of users of services such as interpersonal communication services or hosting services, which allow the storage and, where applicable, dissemination to the public of online content. Depending on the technical characteristics of the service provided, providers of those services have access to different data, and as such, to different types of indications of potentially fraudulent activity. As such, those providers have the capacity to contribute to the collective fight against fraud, including via 'spoofing', by exchanging relevant information with payment service providers, with the aim of preventing and detecting fraudulent uses of interpersonal communication or hosting services. By way of example, relevant information may include the payment account details of traders obtained by providers of online platforms allowing consumers to conclude distance contracts with traders in accordance with Article 30 of Regulation (EU) 2022/2065 related to items of information identified as illegal content by those providers, or information on payment instruments reported as stolen by payment service users to payment service providers. The processing of personal data strictly necessary for the purpose of fraud prevention constitutes a legitimate interest of the interpersonal communication service providers, providers of hosting services, payment service providers and their customers. Providers of interpersonal communication services and of hosting services should be able to exchange personal data with payment service providers to identify fraudulent actors and fraudulent behaviours, where all conditions of Article 6(1)(f) of Regulation (EU) 2016/679 are fulfilled. Furthermore, providers of interpersonal communication services and hosting services should also assist the fight against fraud by exchanging with payment service providers information regarding fraud scenarios, trends and threats identified in relation to the use of their services. In doing so, they may help improve the effectiveness of transaction monitoring mechanisms and the educational campaigns and training on fraud prevention implemented in accordance with this Regulation.

(81) ***Where the relevant conditions, including the requirements of Regulation (EU) 2016/679, for the exchange, on a voluntary basis, of information necessary to prevent and detect fraud are fulfilled***, providers ***of interpersonal communication*** services ***and*** providers ***of very large online platforms and very large online search engines within the meaning of Article 33 of Regulation (EU) 2022/2065*** should ***have in place dedicated communication channels, or enter into information sharing arrangements or systems for effective communication*** with payment service providers***, such as the information sharing arrangements established under Article 29 of Directive (EU) 2022/2555. Such mechanisms should contain robust safeguards in relation to*** confidentiality***, data protection and use of information, in compliance with Regulation (EU) 2016/679.***

(81b) ***Directive (EU) 2022/2555 requires providers of publicly available interpersonal communication services to take appropriate and proportionate technical, operational and organisational measures to ensure the availability, authenticity, integrity and confidentiality of their services. Insofar as the fraudulent manipulation of calling line identification or electronic mail address can be considered to compromise the availability, authenticity, integrity, or confidentiality of those services, such providers should already be required, pursuant to Directive (EU) 2022/2555, to implement measures addressing that risk. Without prejudice to those obligations, providers of publicly available interpersonal communication services should take appropriate organisational and technical measures to detect and prevent the use of their services as a means for impersonation fraud, including by means of manipulation of calling line identification or electronic mail address, where that use aims to induce payment services users to make a payment or to take an action that would compromise the security of the payment account. Any measures taken for the purpose of preventing or detecting the use of these services for impersonation fraud must comply with the rules set out under Regulation (EU) 2016/679 and Directive 2002/58/EC. In particular, those measures should not involve the generalised and indiscriminate monitoring of content of communications or of all traffic data.***

(81c) Regulation 2022/2065 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) lays down fully harmonised rules on the provision of intermediary services in the internal market and on specific due diligence obligations tailored to certain specific categories of providers of intermediary services ('mere conduit', 'caching' and 'hosting' services). In particular, it imposes specific due diligence obligations on online platforms and online search engines, including those designated as very large online platforms or very large online search engines. Such due diligence obligations play an important role in preventing the proliferation of illegal content online, such as financial scams. For instance, hosting services providers are obliged to put in place user-friendly notice and action mechanisms to allow the reporting of illegal content, such as illegal offers of financial services or attempted fraud, to the hosting service. Providers of online platforms are also obliged to address notices from trusted flaggers as a priority. Where, based on the information provided by the payer to the payment service provider, or on other information available to the payment service provider, it can be considered that a fraudulent payment transaction originates in an item of information online, payment service providers should make use of the notification mechanisms referred to in Article 16 of Regulation (EU) 2022/2065 to notify providers of hosting services of the presence on their service of that specific item of information. Where Very Large Online Platforms and Very Large Online Search Engines comply with Article 16 of Regulation (EU) 2022/2065, in particular putting in place notice and action mechanisms that are easy to access and user-friendly, this shall be deemed compliant with the condition in Article 59a(3) to inform the recipients of their services of the procedure for reporting fraudulent actions. Payment service providers should also be able to apply for the trusted flagger status pursuant to Article 22 of Regulation (EU) 2022/2065.

(81e) Regulation (EU) 2022/2065 encourages and facilitates the drawing up of voluntary codes of conduct at Union level to contribute to the proper application of that Regulation, taking into account in particular the specific challenges of tackling different types of illegal content and systemic risks, such as fostering prevention, enhancing security and combating payment fraud and financial scams. The drawing up of a voluntary code of conduct at Union level in the areas covered by this Regulation should also be facilitated.

(81g) The fraudulent promotion and offer of financial services, such as the advertising of credit, insurance, and investment, including cryptoasset, products and services provided by or on behalf of entities which are neither authorised nor registered in accordance with Union law or national law transposing Union law to provide such products and services can be linked with fraud in payments as a result of the deception and manipulation of payment service users' consent into initiating one or a series of payment transactions, or of the theft of sensitive payment data, including personalised security credentials. In order to reduce such fraudulent promotion and offer of financial services, providers of very large online platforms and very large online search engines within the meaning of Regulation (EU) 2022/2065 should request from advertisers of regulated financial services information, such as authorisation or registration numbers, attesting that the provider of the regulated financial service advertised has been authorised or registered to provide such services in a Member State or at Union level. Providers of very large online platforms and of very large online search engines should ensure that their service is not offered for advertising purposes until the advertiser provides the information concerning the registration or authorisation of the entity on behalf of whom the advertisement is made as a regulated financial service provider. This requirement should not amount to an obligation for the providers of very large online platforms and of the very large online search engines concerned to generally monitor the products or services offered by traders through their services, nor a general fact-finding obligation, in particular to assess the accuracy of the information provided by advertisers. However, providers of very large online platforms and of the very large online search engines should, upon receiving from advertisers the information concerning the authorisation or registration of the provider of the advertised regulated financial services, and prior to allowing the advertiser to use their service for the purpose of advertising those regulated financial services, make best efforts to assess whether the information, for the accuracy of which advertisers are responsible for the purposes of this Regulation, is reliable and complete, provided that the assessment can be carried out in a proportionate manner by automated tools. The European Supervisory Authorities – EBA, ESMA, and EIOPA – already maintain public registers of financial service providers under the applicable legislation. Providers of very large online platforms and very large online search engines could use these registers in their efforts to ensure that the information provided by the potential advertiser is reliable and complete.

(81h) Whereas providers of very large online platforms and of very large online search engines within the meaning of Regulation (EU) 2022/2065 have transparency and due diligence obligations with regard to online advertising under that Regulation, this Regulation further specifies how those obligations should apply in the specific case of advertising of regulated financial services. In particular, in order to comply with their obligation to make reasonable efforts to ensure that the information contained in their repositories established pursuant to Article 39 of Regulation (EU) 2022/2065 is accurate and complete, providers of very large online platforms and very large online search engines could use the registers of authorised or registered providers of regulated financial services made available in accordance with relevant Union law, including Directive [PSD3], including the public registers maintained by European Supervisory Authorities.

(81i) Providers of very large online platforms and very large online search engines within the meaning of Regulation (EU) 2022/2065 are required, under that Regulation, to diligently identify, analyse and assess any systemic risks stemming from the design or functioning of their service, including the dissemination of illegal content through their services, such as malicious or fraudulent online content within the meaning of this Regulation. Where applicable, further to that assessment, providers of very large online platforms and very large online search engines should put in place reasonable, proportionate and effective mitigation measures in accordance with Article 35 of Regulation (EU) 2022/2065 to address those risks, under the direct supervision of the Commission. Where, pursuant to Articles 35 of Regulation (EU) 2022/2065, providers of very large online platforms and very large online search engines should put in place mitigation measures related to the risk of fraudulent advertising of regulated financial services which they have identified pursuant to Article 34 of that Regulation, measures put in place in compliance with the obligations set out in this Regulation could be considered to be one of the possible means of ensuring compliance of such providers with Article 35(1), point (e), of Regulation 2022/2065. However, compliance with the obligations set out in this Regulation should not necessarily be construed as sufficient in itself to ensure compliance of such providers with Article 35(1), point (e), of Regulation 2022/2065, and should therefore be without prejudice to further mitigation measures which such providers may be required to put in place.

(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all ***the individual*** circumstances ***of the case***. 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. ***When assessing the possible gross negligence on the part of the*** payment service ***user, all the factual circumstances should be taken into account, for example: innovativeness and complexity of the fraud, means or strategies used by third parties to illegally take over the payment service user's personalised security credentials; whether the payment service user has previously*** fallen victim ▌ to the same ***type of fraud; in the case of a new type of fraud, whether the payment service providers have complied with their obligations under Article 84, including with regard to their most vulnerable groups of customers; whether the payment service user has taken adequate steps in order to properly ensure the confidentiality of their personalised security credentials; any known characteristics of the payment service user that might make the user more likely to fall victim to fraud; whether the payment service providers offered clear, specific and bespoke warnings to the payer; whether the payment service user failed to have regard to specific, directed interventions made by their*** payment service provider***. This list is not exhaustive, cumulative or binding and does not prejudice the discretion of national or EU courts and/or dispute resolution bodies.***

(82a) Taking into account the fact that the term 'gross negligence' is interpreted in very different ways across the Union, the EBA is encouraged to issue guidelines to further specify the factual circumstances that should be taken into account when assessing the possible gross negligence on the part of the payment service user.

(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 ▌ 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 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) ▌It should be possible 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.

(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-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. ▌

(86a) Payment service users should also 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 or otherwise refraining from such execution, such as obligations under this Regulation or Regulation 2024/1624.

(86b) Given that fraud is a criminal activity in accordance with Article 2, point (1), of Directive (EU) 2018/1673, it is therefore considered a predicate offence for the purposes of Regulation (EU) 2024/1624. For that reason, the obligations laid down in that Regulation regarding the reporting of suspicious transactions in accordance with Article 69 of that Regulation, and regarding the obligation to refrain from executing those suspicious transactions in accordance with Article 71 of that Regulation, apply also in cases where a payment service provider knows or suspects that a payment transaction is fraudulent. Those obligations also apply where the payment service provider has reasonable grounds to suspect that a payment transaction is related to criminal activity, such as where the payer's payment service provider has reasonable grounds to suspect that a payment transaction that the payer is initiating may be the result of fraud, or where, before making the funds available to the payee, the payee's payment service provider has reasonable grounds to suspect that a payment transaction that has been or will be credited to its account may be the result of fraud.

(86c) To ensure consistency across the objectives of preventing payment service users' from becoming victims of fraud, compliance with obligations following from Regulation (EU) 2024/1624 with regard to suspicious transactions, and mitigating the impact on payment service users deriving from delays in the execution of legitimate payment transactions or the refusal of such transactions. For that reason, where a payment service provider refuses to execute a payment transaction in accordance with this Regulation, such refusal should be without prejudice to other obligations arising for that payment service provider under Regulation (EU) 2024/1624 with respect to that payment transaction, such as the obligation to report that suspicion to the Financial Intelligence Unit in accordance with Article 69 of that Regulation. In the case of credit transfers, while the outcome of the service ensuring the verification of the payee applied in accordance with Regulation (EU) 2024/886 and Article 50 this Regulation might constitute a relevant element in the payment service provider's monitoring of payment transactions with a view to detecting fraud, that outcome should not in itself be the sole ground for the payment service provider's decision to refuse to execute the payment transaction, with a view to ensuring the right of the payer to proceed with authorising the payment transaction concerned in accordance with Article 5c of Regulation (EU) 260/2012 and Article 50 of this Regulation.

(86d) ***In order to enable the payment service provider to assess whether or not there are objectively justified reasons to suspect that a payment transaction may be fraudulent and therefore to refuse to execute that payment transaction, and in order to limit the impact on payment service users with regard to legitimate payment transactions, the payment service provider of the payer should contact the payer to obtain information necessary for the purpose of such assessment, while remaining in full compliance with the rules on the prohibition of disclosure of suspicions in Regulation (EU) 2024/1624. The payment service provider of the payer should notify the payer of any information or action necessary from the payer for the purpose of its assessment, while providing sufficient information to enable the payer to understand the risks identified by the payment service provider. The payment service provider of the payer should ensure that the payer has at all times appropriate means to contact the payment service provider with a view to providing the information or performing the action requested in that notification, and should make all reasonable efforts to contact the payer before crediting the funds to the account of the payee's payment service provider. In accordance with Article 73 of Regulation (EU) 2024/1624, such communication between the payer's payment service provider and the payer should not at any moment disclose to the payer or, where applicable, the payment initiation service provider, the fact that payment transactions or activities are being or have been assessed in accordance with Article 69 of Regulation (EU) 2024/1624, that information is being, will be or has been transmitted in accordance with Article 69 or 70 of Regulation (EU) 2024/1624 or that an analysis to this effect is being, or may be, carried out.***

(86e) ***Given that, in accordance with Regulation (EU) 260/2012, the amount of an instant credit transfer in euro should be available on the payee's payment account within ten seconds of the time of receipt of the payment order by the payer's payment service provider, the rules requiring the payment service provider of the payer to notify and contact the payer where it suspends the execution of a payment order due to a suspicion of fraud should not apply in the case of instant credit transfers. Those rules should also not apply where the payment service provider of the payer, after notifying and contacting the payer, could nevertheless not obtain the information required before the statutory timeline for crediting the funds to the account of the payment service provider of the payee. In those cases, the payment service provider of the payer should form its assessment as to whether or not there are objectively justified reasons to suspect fraud as well as its decision as to whether or not to refuse to execute the payment order, on the basis of the transaction monitoring mechanism and on any other relevant information available to the payment service provider, but not solely on the basis of the outcome of the service ensuring the verification of payee.***

(86f) 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 objectively justified reasons to suspect fraud. However, any unusual transaction could constitute an early indication of fraud, which should alert the payment service provider and might need to be further investigated. In assessing whether there are objectively justified reasons 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 or on any relevant information available to the payment service provider. Where a decision to refuse or suspend the execution of a payment order is based solely on automated processing, such decision would be permissible only where suitable measures have been applied in order to safeguard the rights, freedoms and legitimate interests of the payment service user.

(86g) ***Where the payment service provider refuses to execute a payment order, the refusal and the reason for the refusal should be communicated to the payer, to the payee's payment service provider and, where applicable, to the payment initiation service provider without undue delay, or, in the case of instant credit transfers, within 10 seconds of the time of receipt of the payment order by the payer's payment service provider, subject to the requirements of Union and national law. In addition, the payment service provider of the payer should inform the payer of the procedure allowing the payer to correct the assessment leading to the refusal, or to reverse that decision. 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. The payment service provider of the payer should not charge fees where it refuses to execute the payment order due to a suspected fraud.***

(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 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 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.

(89a) The obligations in this Regulation regarding open banking interfaces and verification of the payee should not apply as regards payment transactions with electronic money tokens. Extending the application of such requirements to payment transactions with electronic money tokens may impose considerable investments and undue burdens to the entities providing those services, given the high costs associated with the operationalisation of those requirements. Moreover, taking into account the fact that at this stage the transactions with electronic money tokens are not as common as typical payment transactions, there is less urgency and value added in imposing such requirements as regards payment transactions with electronic money tokens.

(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 a maximum 1-day execution time***, unless relevant Union or national law in the field of anti-money laundering and countering terrorism financing provides otherwise***. 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 ***one*** 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 ***one*** business day.

(90a) In order to enable payers to rapidly recover their funds wherever there is high risk that one or a series of payment transactions might be fraudulent, it is appropriate to clarify in this Regulation that, where the payment service provider of the payee has objectively justified reasons to suspect that a payment transaction or series of payment transactions credited or to be credited to its account may be the result of fraud, and where that payment service provider refrains from making those funds available on the payment account of the payee in compliance with its obligation to refrain from executing a suspicious transaction under Article 71 of Regulation (EU) 2024/1624, that payment service provider is able to return the funds credited to its account to the payment service provider of the payer, or to reject the payment transaction or series of payment transactions to be credited to its account by the payment service provider of the payer, as applicable. In order to enhance the protection of payers, it is appropriate to require that, in certain cases where evidence suggesting fraud is stronger, the payment service provider of the payee return the funds to the payment service provider of the payer, or reject the payment transaction or series of payment transactions to be credited by the payment service provider of the payer to its account, as applicable. To avoid excessive de-risking practices, it is appropriate to establish a higher evidentiary threshold according to which that obligation and corresponding liability should apply, where the payment service provider of the payee has strong, consistent and undisputed evidence or indications to conclude, without plausible alternative explanation, that the payment transaction or series of payment transactions are the result of fraud.

(90b) To preserve the trust of payment service users in the reliability of payment services, it is important to ensure that measures aimed at fraud prevention which interfere with the execution of payment orders are sufficiently communicated to the payer, their payment service provider, and, where applicable, the payment initiation service provider, within the timelines applicable to the execution of those payment transactions set out in this Regulation and in Regulation (EU) 2024/886, while remaining in full compliance with rules on the prohibition of disclosure laid down in Regulation (EU) 2024/1624. To prevent the uneven application of those protection and transparency measures in the case of instant credit transfers denominated in Euro and in the case of instant credit transfers denominated in other EU currencies, it is appropriate to establish in this Regulation that, for any instant credit transfer, where, in accordance with this Regulation, the payment service provider of the payee refuses to make the funds available to the payee and, as applicable, returns those funds to the payment service provider of the payer or rejects the payment transaction or series of payment transactions to be credited to its account by the payment service provider of the payer, that payment service provider should notify the payment service provider of the payer of that refusal within ten seconds of the time of receipt of the payment order for that instant credit transfer or series of instant credit transfers by the payment service provider of the payer. Upon receiving such notification, the payment service provider of the payer should immediately restore the payment account of the payer to the state in which it would have been had the transaction not taken place, and, free of charge, inform the payer, and, where applicable, the payment initiation service provider, of the return of the funds, and that the funds have not been made available on the payee's payment account due to fraud prevention measures. In accordance with Article 73 of Regulation (EU) 2024/1624, such communications should not at any moment disclose to the payer or, where applicable, the payment initiation service provider, the fact that payment transactions or activities are being or have been assessed in accordance with Article 69 of Regulation (EU) 2024/1624, that information is being, will be or has been transmitted in accordance with Article 69 or 70 of Regulation (EU) 2024/1624 or that an analysis to that effect is being, or may be, carried out.

(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 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 payment order correctly. ***Without prejudice to its obligation to provide the service ensuring verification of payee,*** the payment service provider of the payer should act with due diligence and verify [redacted] the coherence of the unique identifier, and, where the unique identifier is found to be incoherent ***and therefore the related payment order is not possible to execute***, to refuse ***that*** 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, ***and except where otherwise provided under this Regulation or other relevant Union law,*** to impose liability on the payment service provider in respect of the execution of a payment 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 ***circumstance*** 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 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 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.

(96a) For the purposes of Regulation (EU) 2022/2065, the concept of illegal content should be understood to refer to information, irrespective of its form, that under the applicable EU or national law is either itself illegal, or that the applicable rules render illegal in view of the fact that it relates to illegal activities. Examples include any offer of financial services, including payment services, which is not in compliance with requirements applicable to the offer of such services under this Regulation, Directive XXX [PSD3] or other Union or national law, or content rendered illegal in view of national law on fraud, including offences set out under national law adopted pursuant to Directive (EU) 2019/713.

(96b) Any claim by a payment service provider against other providers, such as electronic communications services providers or providers of intermediary services, for financial damage caused in the context of fraud should be made in accordance with national law.

(96c) With regard to providers of intermediary services, Regulation (EU) 2022/2065 sets up a fully harmonised framework for the conditional exemption from liability of those providers, under certain conditions and as interpreted by the Court of Justice of the European Union. In order to benefit from the exemption from liability for hosting services under Regulation (EU) 2022/2065, providers of hosting services including online platforms, should remove illegal content or disable access to it, expeditiously, upon obtaining actual knowledge or, in the case of claims for damages, upon becoming aware of the content, in particular in cases in which the provider of hosting services has been made aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question. In particular with regard to providers of hosting services as defined in Article 3(g)(iii) of the Digital Services Act, where those conditions for exemption from liability under Article 6(1) of Regulation (EU) 2022/2065 are not met, and hosting service providers become liable for content stored in their services, and where that content gave rise to one or a series of unauthorized payment transactions or fraudulent authorized payment transactions within the meaning of this Regulation, payment service providers should be able to obtain compensation from hosting services providers for the amount refunded to their customers for those transactions under this Regulation.

(96d) Nothing in this Regulation should be interpreted as a general obligation placed on providers of hosting services to monitor the information which they transmit or store, nor as requiring those providers to actively seek facts or circumstances indicating illegal activity, such as the impersonation of a payment service provider.

(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 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,[17] 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.

[17] 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).

(98) As acknowledged in the Communication from the Commission on a Retail Payments Strategy for the EU, the good functioning of EU payments markets***, including the security of payments and the protection of payment service users against fraud,*** is of substantial public interest. ***For that reason***, when it is necessary in the context of this Regulation for the provision of payment services and for ▌ compliance with this Regulation, payment service providers and ▌ operators ***of payment systems and payment schemes*** 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***, in accordance with Articles 9(2), point (g), and 10(2), point (g) of those Regulations respectively***. 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.

(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 ***important*** role in that detection. It is therefore appropriate to require ***both the payer's*** payment service ***provider and the payee's payment service provider*** 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 in the case of instant credit transfers means in real-time. The payment service provider of the payee should carry out such transaction monitoring before making the funds available to the payee. Where a payment service provider fails to comply with its obligations with respect to the application of transaction monitoring to one or a series of payment transactions, and where that payment transaction or series of payment transactions were initiated through fraudulent means, or otherwise as a result of fraud, the full amount of that payment transaction or series of payment transactions should be refunded to the payer by their payment service provider. Where the payment service provider that failed to apply transaction monitoring is the payment service provider of the payee, it should refund the payment service provider of the payer for the amount refunded by the latter to the payer.***

(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) ▌Payment service providers should be able to process information about their customers' transactions and their payment accounts ***to the extent necessary to ensure that transaction monitoring mechanisms effectively enable them to detect and prevent fraud, in particular by detecting atypical behaviour of the payment service user that might indicate a potentially fraudulent transaction or use of the payment account.. Transaction monitoring carried out by*** payment service providers ***, might***, ▌ to the ***extent*** necessary to ***achieve the purpose of*** detecting ***fraud, include the processing of information exchanged by means of the*** service ***ensuring the verification*** of the ***payee or in the context of information sharing arrangements established in accordance with this Regulation or other relevant Union law***.

(102a) Payment service providers should store data processed for the purpose of complying with their obligations with respect to transaction monitoring and fraud information sharing only for as long as necessary for those purposes, and in any event, only for a maximum of five years after the termination of the customer relationship. The revised FATF Recommendations demonstrate that, in order to be able to cooperate fully and comply swiftly with information requests from competent authorities for the purposes of the prevention, detection or investigation of money laundering and terrorist financing, obliged entities should maintain, for at least 5 years, the necessary information obtained through customer due diligence measures and the records on transactions. Accordingly, Regulation (EU) 2024/1624 establishes that the retention period applicable to personal data processed in accordance with that Regulation, including as regards information processed in the context of information sharing partnerships established under Article 75 of that Regulation, should be fixed at 5 years after the end of a business relationship or an occasional transaction. Given that fraud is considered to be a criminal activity, in accordance with Article 2, point (1), of Directive (EU) 2018/1673, and is therefore considered a predicate offence for the purposes of Regulation (EU) 2024/1624, it is appropriate to establish that a maximum retention period applicable to personal data processed in accordance with this Regulation should also be fixed at 5 years after the end of a business relationship or an occasional transaction, in order to ensure legal certainty and consistency across financial crime preventative and detection measures.

(103) Fraud ▌ 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***, as well as of fraud intelligence as complete and up to date as possible***. Often***,*** one payment service provider does not have ***full overview of*** all elements ***and indicators*** that could lead to timely ▌ detection ***of*** potentially fraudulent activity ***in a given*** payment ***transaction. The exchange of*** information ***among*** payment service providers ***can increase the possibilities for*** better ***detecting potential fraud and protecting*** payment ***service users. For that reason***, payment services providers should, for the purpose of transaction monitoring, make use of payment fraud data shared by other payment services providers***,*** ***and share payment fraud data with other payment service providers*** on a multilateral basis ***in the framework of*** information sharing arrangements. ***Where the sharing of information involves the processing of personal data***, ***such sharing should be limited to the types of personal data which*** payment service providers ***can process for the purpose of monitoring transactions*** in accordance with ***this*** Regulation***. However, environmental and behavioural characteristics, which are typical of the payment service user*** in the ***circumstances of a normal use of the personalised*** security ***credentials, should not be shared. Data shared should relate*** to the ***specific payment transactions for which the payment service provider has a suspicion of fraud, and not to connected previous or subsequent transactions.*** Payment service providers should ***also share the objectively justified reasons which have led to the suspicion of fraudulent activity with respect to that particular payment transaction, and, where that*** payment ***transaction is associated with a potentially fraudulent item of*** information ***stored by a provider of hosting services,*** information ***concerning the notification made to that provider of hosting services.***

(103a) Information sharing should be subject to robust state-of-the-art safeguards relating to confidentiality, data protection and use of information, such as pseudonymisation and encryption, access and user control, and should be in accordance with Regulation (EU) 2016/679. Before concluding an information sharing arrangement, payment service providers should carry out a data protection impact assessment, in accordance with Article 35 of that Regulation. Where the data protection impact assessment indicates that, in the absence of safeguards, security measures and mechanisms to mitigate the risk, the processing would 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. 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 also lay down the roles and responsibilities of all involved payment service providers in accordance with data protection rules, including in the case of joint controllership.

(103b) Payment service providers are able to exchange data related to payment transactions where there is a suspicion of fraud with other participants of information sharing partnerships established in accordance with Article 75 of Regulation (EU) 2024/1624, including competent authorities such as Financial Intelligence Units (FIUs), supervisory authorities and any public authority that has the function of investigating or prosecuting money laundering, its predicate offences or terrorist financing, or that has the function of tracing, seizing or freezing and confiscating criminal assets, in accordance with fundamental rights and judicial procedural safeguards. Payment service providers are also able to share with other payment service providers and other participants, including public authorities, data related to threats to the security of their ICT systems, including where 'spoofing', phishing and malware are used to commit fraud against payment service users, in the context of information sharing arrangements on cyber threat information and intelligence established under Article 45 of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector. As such partnerships or arrangements already provide adequate frameworks for the involvement of public authorities, including law enforcement authorities, in the voluntary sharing of data related with fraud, subject to adequate safeguards, it is not considered necessary to create an additional regime for such exchange under this Regulation.

(103c) Where a payment service provider participates in information sharing partnerships or arrangements established in accordance with Article 75 of Regulation (EU) 2024/1624 and Article 45 of Regulation (EU) 2022/2554, and where those information sharing partnerships or arrangements enable the payment service provider to exchange the data necessary for the purposes of detecting and preventing fraud in accordance with this Regulation, the sharing of data within the framework of those information sharing partnerships should be considered sufficient to ensure compliance by the payment service provider with its obligations under this Regulation to share payment fraud data in the framework of information sharing arrangements. Where payment service providers participate in those information sharing partnerships or arrangements for the purpose of complying with obligations under this Regulation, they should be allowed to process personal data exchanged in the context of such partnerships or arrangements for the purpose of complying with the transaction monitoring obligations set out in this Regulation.

(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 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.

(105a) When developing measures to combat fraud in the area of payments services, it is particularly important to conduct appropriate consultations with relevant stakeholders in order to exchange best practices and share experiences. Those consultations should build on input from public- and private-sector experts with proven knowledge and experience in the areas concerned. To that end, the Commission should establish a platform on combating fraud (the 'Platform'). The Platform should be composed of experts and may include, for example, representatives of relevant Union bodies, national competent authorities, payment service providers, technical services providers, providers of online platforms, telecommunications providers, internet service providers, experts representing different payment systems or schemes, merchants, consumer organisations, and dispute-resolution bodies.

(105b) The Platform should be constituted in accordance with the applicable horizontal rules on the creation and operation of Commission expert groups, including with regard to the selection process. The selection process should aim to ensure a high level of expertise, geographical and gender balance, as well as a balanced representation of relevant knowledge and experience, taking into account the specific tasks of the Platform. During the selection process, the Commission should carry out an assessment in accordance with those horizontal rules to determine whether potential conflicts of interest exist and should take appropriate measures to prevent or address any such conflicts.

(105c) The Platform should advise the Commission on developing and monitoring of the implementation of legal acts aimed at combatting fraud in the area of payment services. For the purpose of drawing up a voluntary code of conduct to foster prevention, enhance security and combat payment fraud and financial scams, the platform should provide recommendations to the Commission and the European Board for Digital Services. The Platform should also share information on and analyse trends in fraud in the area of payment services, as well as share information on measures to combat fraud in the area of payments services, including mitigation measures, and on ways to improve cross-border and cross-sectoral cooperation on the means of combatting fraud in the area of payment services. The Platform should carry out its tasks in accordance with the principle of transparency. It should also take into account the work of existing initiatives to combat payment fraud, avoiding duplication, and work closely with them.

(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. 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, ***appropriate*** information about fraud, giving them clear messages and warnings, helping them to react properly when exposed to potentially fraudulent situations. The EBA should ***be encouraged to*** develop guidelines about the different ▌ programmes to be developed by payment service providers on payment fraud risks, taking into account the ever-changing nature of fraud-related risks***,*** ***where it deems necessary to achieve consistency of such programmes across the Union***.

(106a) Awareness about fraud threats is essential to enhance the level of protection of payment service users against such threats, and therefore their level of confidence in the use of payment services across Union, in particular in light of the rapid change in the techniques and strategies deployed by fraudsters. Member States can play a crucial role in ensuring the collective levelling of awareness and preparedness of citizens in this regard, beyond the individual information supplied on this matter by service providers to their customers. Directive (EU) 2022/2555 already requires Member States to develop national cybersecurity strategies, in the context of which specific policies should be adopted with the aim of promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research and development initiatives, as well as guidance on good cyber hygiene practices and controls, aimed at enhancing the level of awareness and preparedness of citizens, stakeholders and entities against cybersecurity risk, including techniques used to carry out fraud, such as phishing, spoofing, malware and other forms of social engineering. Furthermore, Directive (EU) 2019/713 requires Member States to establish or strengthen policies to prevent fraud and counterfeiting of non-cash means of payment and measures to reduce the risk of such offences occurring, including attempts to commit fraud such as phishing and skimming, by means of information and awareness-raising campaigns and education programmes. In compliance with their obligations under those Directives, Member States should develop and keep up to date permanent and adequate measures to raise awareness among the public about the existing and emerging patterns of payment fraud, procedures to be followed in accordance with this Regulation in order to identify and report fraud attempts and the rights and obligations of payment service users with regard to fraud under this Regulation. Member States should inform the Commission of the measures adopted.

(106b) Member States should ensure that sufficient funding is available for such awareness raising and education measures, and that they are adequately targeted, in particular to the needs and interests of vulnerable consumer groups, including young and elderly people and those with low digital skills. Payment service providers, providers of interpersonal communication services as defined in Article 2(4), point (b), of Directive (EU) 2018/1972, and providers of very large online platforms and very large online search engines within the meaning of Regulation (EU) 2022/2065 should cooperate with the Member States in the development and updating of such fraud awareness campaigns, including by providing information on fraud threats and patterns identified in their services, and best practices in terms of users' awareness. Such cooperation should be free of charge, within reasonable and proportionate terms.

(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 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.

(107b) Requirements for strong customer authentication should not be changed substantially from the existing requirements under Directive (EU) 2015/2366. Strong customer authentication will continue to be based on two or more elements categorised as knowledge, possession and inherence, that are independent from each other. The category inherence relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. At least two of the elements used need to come from different categories. To allow for innovations in authentication technology, an exception to that principle foresees the usage of two elements from the category inherence, if this does not lower the level of security. To ensure a high level of security and the uniform application of this exception by national competent authorities, EBA should develop guidelines on how to assess the independence of the two elements in this case.

(108) SCA should not be circumvented***, in particular*** 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 of the*** payment ***order, and not also 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 transaction 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 ***SCA*** 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 ***SCA***, 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, ***excluding the unconditional right to a refund, which should apply only to direct debits***.

(109a) In the interest of establishing a level-playing field among different payment instruments, it should be possible to initiate one or several recurring credit transfers, including of varying amounts, without the obligation to apply strong customer authentication where such credit transfers are initiated by the payment service provider of the payer following a request from the payee, provided that certain cumulative conditions are met. In particular, this should be possible where the request from the payee is based on the payee's agreement with the payer which sets out the conditions regarding frequency of payments and amounts to be paid, where the payer sets up an agreement with its payment service provider which is subject to strong customer authentication and which instructs the provider to execute the respective credit transfers in line with the agreement of the payer with the payee, and where the initiation of the respective credit transfers by the payer's payment service provider does not require any additional action from the payer. To ensure equivalent safeguards, the provisions concerning refunds and requests for refunds applicable to payment transactions initiated by or through a payee should apply to credit transfers falling under this framework under the same conditions as those applicable to merchant-initiated transactions. In addition, to promote unhindered innovation and accelerate broader availability of efficient payments methods to payers and payees at the point of interaction, it is necessary to allow the possibility to initiate one or several recurring credit transfers under that framework as of the date of entry into force of this Regulation.

(110) To improve financial inclusion, and in line with Directive (EU) 2019/882 of the European Parliament and of the Council[1] 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 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 ***they lack capability to perform*** 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 be free of charge and*** should not depend on one single technology, device or mechanism, or on the possession of a smartphone ***or another smart device***.

(111) European Digital Identity Wallets implemented under Regulation (EU) No 910/2014[18] 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. ***Pursuant to Art. 5f(2) of Regulation (EU) No 910/2014, payment service providers will be under an obligation to accept the use of the EU Digital Identity Wallets for supporting the fulfilment of SCA requirements for online identification for the purposes of account login and of initiation of transactions in the field of payment services. The EBA should be tasked with the drafting of regulatory technical standards which should specifically take into account the use of EU Digital Identity Wallets to support the fulfilment of SCA requirements for the purposes above.***

[18] 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).

(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 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 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 ***such*** 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.

(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 ***or payment transactions initiated by legal persons***, 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 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 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 ***SCA*** 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 should be held liable for ***direct*** financial ***damage*** caused to payees***,*** to the payment service providers of the payees or of the payers ***for, and proportionate to, their failure, within the remit of their contractual relationship, and not exceeding the amount of the transaction in question, to provide the services that are necessary to enable*** the application of strong customer authentication.

(121) Member States should ***ensure that*** competent authorities ***designated by Member States under Article 18 of Directive 2013/11/EU perform the functions set out in Articles 19 and 20 of that Directive regarding*** dispute resolution ***entities established on their territories, which intend to qualify as ADR entities for the settlement of disputes concerning the rights and obligations under this Regulation***.

(121d) 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 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, those powers should already take effect at the investigation stage if there is a reasonable suspicion (facts justifying the assumption) of unauthorised business operations.

(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 the Council[1] 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[2], to resolve disputes before resorting to a court. ***For contractual consumer-to-business disputes regarding the purchase of goods or services, Directive 2013/11/EU ensures that consumers and businesses in the Union have access to quality-certified out-of-court dispute resolution*** entities ***that comply with the quality requirements set out in Directive 2013/11/EU. Participation in alternative dispute resolution procedures for the settlement of*** disputes ***between payment service providers and consumers*** concerning rights and obligations pursuant to this Regulation ***should be mandatory for payment service providers***. ***That would allow consumers, who do not have the same means and resources as legal persons, to enforce their rights under this Regulation, to have access to more expedient and cheaper enforcement means. However, consumers should not be forced to participate in such alternative dispute resolution procedures.***

(122a) In accordance with Directive 2013/11/EU, the right to an effective remedy and the right to a fair trial are fundamental rights laid down in Article 47 of the Charter of Fundamental Rights of the European Union. Therefore, ADR procedures should not be designed to replace court procedures and should not deprive consumers or traders of their rights to seek redress before the courts. This Regulation should not prevent parties from exercising their right of access to the judicial system. In cases where a dispute could not be resolved through a given ADR procedure whose outcome is not binding, the parties should subsequently not be prevented from initiating judicial proceedings in relation to that dispute. Member States should be free to choose the appropriate means to achieve this objective. They should have the possibility to provide, inter alia, that limitation or prescription periods do not expire during an ADR procedure.

(123) Consumers should be entitled to enforce their rights in relation to the obligations imposed on payment ▌ service providers under this Regulation through representative actions in accordance with Directive (EU) 2020/1828 of the European Parliament and of the Council'[19].

[19] 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).

(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[20] and which act independently from the payment service providers. Member States should notify the Commission which authorities have been designated, with a clear description of their tasks.

(124a) In light of the fact that certain provisions in Directive (EU) 2015/2366, such as the ones on ex ante transparency of costs and execution time, were designed having in mind traditional electronic payments and did not take into account the specific characteristics of the use of distributed ledger technology or similar technology for payment transactions with electronic money tokens, it is important to specify whether those requirements apply to payment transactions with electronic money tokens, and to introduce transitional provisions in this regard.

[20] 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).

(124b) It is necessary to enhance convergence of powers at the disposal of competent authorities so as to pave the way towards an equivalent intensity of enforcement across the integrated payments market. Competent authorities should be granted all the supervisory, investigatory and sanctioning powers necessary to ensure compliance with this Regulation. This Regulation should therefore lay down a common minimum set of powers competent authorities should be entrusted with, coupled with adequate resources to guarantee supervisory effectiveness. In order to protect consumers and ensure adequate information of the market at any time, competent authorities should be empowered to adopt timely supervisory measures, such as suspending or prohibiting the provision, marketing and advertising of services, or issuing public notices to warn the public about an actual or suspected infringement of this Regulation. Competent authorities should use those powers in particular when the infringement takes the form of unauthorized payment services, false or misleading information disseminated through the payments market, and more in general when a payment service provider or third party involved in the provision of payment services has failed to fulfil its obligations under this Regulation. Where information published by competent authorities through public notices was to appear inaccurate, incomplete or its underlying circumstances incorrect, competent authorities should promptly rectify it through the same communication channels used to inform the public.

(124c) In a digital environment competent authorities should be able to stop infringements of this Regulation swiftly and effectively, notably where the infringer conceals his identity or relocates within the Union or to a third country in order to avoid enforcement. In cases where there is a risk of serious harm to the interests of consumers, the competent authorities should be able to adopt interim measures, including the removal of content from an online interface or ordering the explicit display of a warning to consumers when they access an online interface. Such measures should not go beyond what is necessary to achieve the objective of bringing to an end or prohibiting the infringement of this Regulation.

(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 ▌ 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 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 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, [redacted] 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 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 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***, which are applied in accordance with national law,*** 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 ***or other administrative measures*** 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 where relevant to remedy the situation in the case of infringement ***of this Regulation***. 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 ***as well as information on the right to appeal them and the outcome of such an appeal*** 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 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 ***with the aim to further specify the fee information that payment card schemes and processing entities must disclose to acquiring payment service providers;*** to update ***the amount*** up to which a payer may be obliged to bear ▌ losses relating to ▌ unauthorised payment transactions resulting from the ***loss, theft or*** misappropriation of a payment instrument ***or personalised security credentials; to adjust the rules applicable to payment transactions with electronic money tokens in light of technological and market developments; and to specify the criteria and factors to be taken into account by the EBA when determining certain conditions related to temporary intervention powers***. 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. ▌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, ***the EBA should*** 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 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) ***To facilitate cross-border cooperation on the enforcement of this Regulation,*** the Annex to Regulation (EU) 2017/2394 of the European Parliament and of the Council[8] should be amended to include a reference to this Regulation ▌.

[8] 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 2006/2004 (OJ L 345, 27.12.2017, p. 1–26).

(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 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 ***27*** months after the date of entry into force of this Regulation, thus granting payment service providers enough time to take the necessary steps to 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. ***Seven*** 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 [redacted] further solutions to combat fraud ***and the appropriateness and impact of the rules on the extent of situations where a consumer has a refund right for authorised transactions***. ***However*** regarding ***other topics, namely the charging practices for payment services, the obligations imposed on electronic communications services providers and on providers of hosting services on payments fraud prevention,*** the scope of this Regulation, ***the appropriateness and the impact of the rules set out in this Regulation with regard to payment transactions with electronic money tokens***, it is appropriate for a review to take place earlier ***than 7*** years***,*** after entry into ***force***, given the ***fundamental*** importance attached to ***those topics for the functioning of a competitive, innovative and secure payments market in the Union***[22]. That review of scope should consider both the possible 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.

[22] 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).

(144a) In view of the increasing relevance of virtual IBANs being used for legitimate business purposes within the Union, it is essential to enhance legal certainty and ensure compliance with Regulation (EU) No 260/2012. It is therefore necessary to clarify that virtual IBANs are subject to the same rules as IBANs, containing the elements specified by the International Organisation for Standardisation (ISO). Regulation (EU) No 260/2012 should be amended accordingly. In addition, virtual IBANs are permissible as valid payment account identifiers where the use of an IBAN is required. Considering the risks and challenges posed by virtual IBANs, including from an anti-money laundering perspective, on the one hand, and their benefits, on the other, the Commission should assess and conclude in its report whether it is necessary to introduce any further measures regulating virtual IBANs at Union level and, if appropriate, submit a legislative proposal together with the report.

(144b) In keeping with the principles of better regulation, this Regulation should be reviewed for the appropriateness and the impact of the rules set out in Titles II and III of this Regulation with regard to payment transactions with electronic money tokens. In its review, the Commission should assess whether, given developments, it would be desirable, to extend the requirements on the verification of the payee and open banking under this Regulation to payment transactions with electronic money tokens.

(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.

(145a) Regulation (EU) No 2023/1114 provides that certain firms subject to Union legislative acts on financial services should be allowed to provide all or some crypto-asset services without being required to obtain an authorisation as a crypto-asset service provider if they notify their competent authorities with certain information before providing those services for the first time. In order to establish a comprehensive list of those firms it is necessary to amend Regulation (EU) No 2023/1114 and to also provide that payment institutions which are authorised under Directive XXX [PSD3] should be able to provide crypto-asset services in relation to e-money tokens for the purposes of providing payment services, where such crypto-asset services are deemed equivalent to those payment services.

(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.***

(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 Council[23] and delivered an opinion on [XX XX 2023][24],

---

[23] 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).

[24] OJ C […], […], p. […].

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 ▌, as regards:

   (a) the transparency of conditions and information requirements for payment services ▌;

   (b) the respective rights and obligations of payment ▌ service users, and of payment ▌ service providers in relation to the provision of payment services ▌.

2. Unless specified otherwise, any reference to payment services shall be understood in this Regulation as meaning payment ▌ services ***as referred to in Annex I of [PSD3]***.

▌

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[25], including branches thereof where such branches are located in the Union, whether the head offices of those are 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.

[25] 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).

1a. 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, 88a, 89, 91 and 93;

(b) operators of payment systems and payment schemes, for the purposes of Articles 31, 80, 91 and 93, payment schemes for the purpose of Articles 31a 58 and processing entities for Article 31a;

(c) providers of electronic communications services as defined in Article 2(4), point (b), of Directive (EU)2018/1972, for the purposes of Articles 59, 59a, 84, 88a, 91 and 93;

(ee) providers of electronic communications services as defined in Article 2(4), of Directive (EU)2018/1972, for the purposes of Article 88a;

(ef) providers of hosting services, for the purposes of Articles 59a, 78 and 91;

(eg) providers of very large online platforms and of very large online search engines within the meaning of Article 33 of Regulation (EU) 2022/2065 for the purposes of Articles 59a, 59b, 84 and 89a;

(eh) original equipment manufacturers of mobile devices for the purposes of Article 88a.

2. This Regulation does not apply to the following ▌ :

(a) payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention;

(a1) payment transactions made exclusively in electronic money tokens directly from the payer to the payee, without any intermediary intervention;

(b) payment transactions from the payer to the payee through a commercial agent, ▌ provided that ***the*** 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***; and***

(ii) such agreement gives the ***commercial agent*** a real ***scope*** to negotiate with the ***payer or payee*** or conclude the sale or purchase of goods or services;

(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;

(e) services where ▌ retail stores ***agree to provide cash*** 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 ▌ ;

(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;

(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 ***or physical vouchers of similar nature***;

(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 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;

(ha) payments transactions carried out by a crypto-asset service provider intermediating between a buyer and a seller where electronic money tokens are exchanged for other electronic money tokens or for crypto-assets, as well as the exchange of electronic money tokens for funds, including electronic money tokens, or crypto-assets carried out by a crypto-asset service provider acting in its own name as buyer or seller of those electronic money tokens;

I

(j) services based on specific payment instruments***, including electronic money-based instruments,*** that meet one of the following conditions:

(i) instruments allowing the holder to acquire goods or services only in the premises***, including physical premises or online stores,*** 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***, including instruments restricted to be used in transactions between payment service users who are not consumers***;

(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***, and which cannot be converted into cash***;

(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[26], or 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 ***60*** and:

- the cumulative value of payment transactions for an individual subscriber does not exceed EUR ***360*** 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 ***360*** per month;

[26] 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).

(l) payment transactions carried out between payment service providers, their agents or branches for their own account;

(la) payment transactions carried out between crypto-asset service providers or their branches for their own account;

(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.

(n) professional physical transport of banknotes and coins, including their collection, processing and delivery;

(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 ***(b)(v)*** 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 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 ***(b)(v)*** and point ***(e)(viii)*** and Article 24, point (a), and Title III, except for Article 28(2) and (3), Articles ***50, 57,*** 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 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 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 ***home Member State as defined in Article 2, point (1), of Directive XXX [PSD3];***

(2) 'host Member State' means ***host*** Member State ***as defined in Article 2, point (2), of Directive XXX [PSD3]***;

(3) 'payment service' means any business activity set out in Annex I ***of Directive XXX [PSD3]***;

(4) 'payment institution' 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 ***execution*** of a payment transaction ***as defined in Article 2, point (6) of [PSD3]***;

(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 ***or allows*** a payment order from that payment account, or, where there is no payment account, a ***natural or legal*** 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 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 ***can be*** used for the execution of one or more payment transactions and allows for sending and receiving funds to and from third parties;

(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 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 ***payment service user***;

(20) ‘payment initiation service’ means a service to place a payment order at the request of the ***payment service user*** with respect to a payment account held at another payment service provider;

(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 several account servicing payment service providers ***that are accessible online in order to provide a service of aggregation or consolidation of payment account data to the payment service user or to transmit the data to another entity that will provide that service to the payment service user***;

(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;

(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 ***money remittance as defined in Article 2(22) of PSD3***;

(27) ‘direct debit’ means a payment service for debiting a payer’s payment account, 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 ***executed*** immediately***, 24 hours a day and on any calendar day***;

(30) ‘funds’ means central bank money issued for retail use, scriptural money and electronic money***, including electronic money tokens***;

(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 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***, although not being payment services,*** 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;

(38) ‘sensitive payment data’ means data which can be used to carry out fraud, including personalised security credentials;

(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 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 ***other than instant credit transfers***;

(44) 'agent' means ***an agent as defined in Article 2, point (28), of Directive XXX [PSD3]***;

(45) 'branch' means a ▌ branch ***as defined in Article 2, point (29), of Directive XXX [PSD3]*** ;

(46) 'group' 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 ▌ 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;

(53) ‘commercial trade name’ means the name which is commonly used by the payee ***in the trade and marketing of its business*** to identify itself to the payer;

(54) ‘ATM deployer’ means ***an ATM deployer as defined in Article 2, point (38), of Directive XXX [PSD3];***

(56) ‘merchant-initiated transaction (MIT)’ means a payment transaction where the payer has given a mandate authorising 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, where the mandate is based on an agreement between the payer and the payee for the provision of products or services, and where those transactions do not need to be preceded by a specific action of the payer to trigger their initiation by the payee;

(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 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;

(58) 'aggregated mid-market exchange 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;

(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 this Regulation and compelling the natural or legal person to return to compliance with the infringed provisions or decisions;

(60) 'electronic money token' means an electronic money token as defined in Article 3(1), point (7), of Regulation (EU) 2023/1114;

(61) 'crypto-asset service' means a crypto-asset service as defined in Article 3(1), point (16), of Regulation (EU) 2023/1114;

(62) 'providing transfer services for crypto-assets on behalf of clients' means providing transfer services for crypto-assets on behalf of clients as defined in Article 3(1), point (26), of Regulation (EU) 2023/1114;

(63) 'crypto-asset service provider' means a crypto-asset service provider as defined in Article 3(1), point (15), of Regulation (EU) 2023/1114;

(64) 'self-hosted address' means a self-hosted address as defined in Article 3, point (20), of Regulation (EU) 2023/1113;

(65) '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;

(66) 'payment card scheme' means a payment card scheme as defined in Article 2, point (16), of Regulation (EU) No 2015/751;

(67) 'processing' means processing as defined in Article 2, point (27), of Regulation (EU) No 2015/751;

(68) 'processing entity' means a processing entity as defined in Article 2, point (28), of Regulation No (EU) 2015/751.

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.

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. ***Payment transactions*** shall be made in the currency agreed between the parties.

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 the payer shall disclose to the payer all charges and the exchange rate to be used for converting the payment transaction.

   For the purposes of the first subparagraph, and of Articles 7, 13(1), point (f) and 20(c), point (v), of this Regulation, the aggregated mid-market exchange rate used shall accurately reflect the market, with a maximum delay of 10 minutes or, for currencies where this is not possible, it shall 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.

3. The payer shall be given the possibility to agree to the currency conversion service on that basis.

Article 6

Information on additional charges or reductions

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***.

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 comprehensible manner*** prior to the initiation of the payment transaction.

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***, including those*** referred to in Article 38 of Directive (EU) [PSD3]**,** shall ***display at the ATM*** to their customers information on any charges ***for*** the withdrawal ***payable by the customer, including, if applicable, conversion charges in accordance with Article 5(4). The information shall be displayed in a clear, neutral and comprehensible manner prior to the initiation*** of the ***payment transaction. 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.

Article 8

Charges for information

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

Derogation from information requirements for low-value payment instruments and electronic money

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 ***that does not exceed EUR 300*** or store funds that do not exceed EUR ***300*** 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 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 provide the payer with a possibility to verify the amount of funds stored.

2. By way of derogation from paragraph 1, the spending and storing limits for prepaid payment instruments shall not exceed EUR 500.

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

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***, in an official language of the Member State where the payment service is offered or in any other language agreed between the parties.

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.

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) ***where the payee's payment service provider is located outside the Union,*** the estimated time for the funds of credit transfers and money remittance transactions to be received by ***that*** payment service provider ▌ ;

   (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 ***monetary amount in the currency of the payer's account and as a*** percentage mark-up over ***an aggregated mid-market exchange rate as referred to in Article 5(4). That mark-up and any other*** applicable ***charges shall be disclosed to the payer prior to the initiation of the payment transaction***;

(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.

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;

(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

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 ***and, where available to the payment service provider and if different from the commercial trade name, the payee's legal 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 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.

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 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***, neutral*** and comprehensible ***manner***, in an official language of the Member State where the payment service is offered or in any other language agreed between the parties.

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 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 ▌ 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;

(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 ***consent*** to execute a payment transaction and withdrawal of such ***consent*** 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;

(vii) ***the*** spending limits for the use of ***each*** payment instrument in accordance with Article 51(1) ***with information on the length of a delay for any resulting increase in spending limits to come into effect and description of how the payment service user can modify the spending limits and adjust or opt out of the application of a delay period***;

(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;

(4) an ATM ***deployer***;

(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 ***an aggregated mid-market exchange rate as referred to in Article 5(4). That mark-up and any other*** applicable ***charges, also expressed as a monetary amount in the currency of the payer's account, shall be disclosed to the payer prior to the initiation of each payment transaction***;

(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 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) ▌ 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***, 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 Article 59 ***or*** of any unauthorised or incorrectly initiated or executed payment transaction ▌, 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 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

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 *to* the framework contract

1. The payment service provider shall propose any changes ***to*** the framework contract**,** ***including to*** 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 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 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.

▌

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 ***3*** 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 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 ***3*** 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 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***, prior to the initiation of the payment transaction,*** 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 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 ***and, where available to the payment service provider and if different from the commercial trade name, the payee's legal name***;

   (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 ***a frequency to be determined by the payer of up to 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.

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;

   (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 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 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 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 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 ***that does not exceed EUR 300***, or store funds which do not exceed EUR ***300*** at any time, payment service providers may agree with their payment service users that:

   (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.

1a. ***By way of derogation from paragraph 1, the spending and storing limits for prepaid payment instruments shall not exceed EUR 500.***

2. Articles 56 and 60 shall apply also to electronic money, except where the payer's 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.

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.

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 between the electronic money issuer and that person.

8. A payment institution ***that issues*** electronic money ▌ 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 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 ***in*** 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.

I

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.

5a. Paragraphs 1, 2, 3 and 5 shall apply to operators of payment schemes. Those paragraphs shall not apply to operators of payment systems and payment schemes composed exclusively of payment service providers belonging to the same group.

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 service provider with full reasons for such rejection.

7. ▌ Member States shall designate a competent authority ▌ to ensure ***compliance with*** paragraphs ***1, 2***, 3, 5 and 6 ***as applicable*** by payment systems ***and payment schemes*** governed by their national law***, except for cases where those requirements are enforced by the Eurosystem or central banks of non euro area Member States as part of the oversight of the operations of those payment systems or schemes, such as payment systems subject to Regulation (EU) 2025/1355***.

Article 31a

Transparent practices of payment card schemes, processing entities and acquirers

1. Operators of payment card schemes and processing entities shall ensure that the fees imposed on payment service providers providing acquiring services are categorised and disclosed in a clear and consistent manner allowing for the comparability of billing categories between schemes and processing entities, based on at least the following categories:

interchange fees;

processing fees; and

scheme fees of which:

- mandatory fees;

- fees linked to a specific behaviour or to the use or non use of a technology; and

- fees related to optional services.

The categories of fees shall be clearly defined.

That information shall be disclosed to payment service providers providing acquiring services in a manner ensuring full clarity as to which fees correspond to which services. The information shall be as specific as possible and, where possible, distinguish the fees applied according to the card category, the sales channel, the transaction volume and value of the merchant and the geographical location.

2. Payment service providers providing acquiring services shall use the information disclosed under paragraph 1 when fulfilling their obligations set by Articles 9 and 12 of Regulation (EU) 2015/751.

3. For the purposes of paragraph 1, operators of payment card schemes and operators of processing entities shall:

- communicate any new fees and any change in scheme and processing fees unambiguously in a transparent and consistent manner to the payment service providers providing acquiring services no later than 6 months prior to their implementation;

- maintain a single EU public repository of their scheme and processing rules and fees, according to the categories of fees referred to in paragraph 1.

4. The Commission shall adopt a delegated act in accordance with Article 106 to supplement this Regulation by further specifying the information to be disclosed to payment service providers providing acquiring services under paragraph 1. The Commission shall adopt that delegated act by [OP please insert the date= 15 months after the date of entry into force of this Regulation.

Article 32

Provision by credit institutions of payment accounts to payment institutions

-1. Credit institutions shall provide access to payment accounts to payment institutions, their agents and applicants for authorisation as a payment institution 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 ***may*** refuse to open or ***may*** close a payment account for a payment institution for its agents or ▌ for an applicant for ***an authorisation*** as a payment institution ***only*** in the following cases:

   (a) the ***opening or maintaining such a payment account would result in an infringement of Regulation (EU) 2024/1624 of the European Parliament and of the Council[27];***

   (b) there is or has been a ***material*** breach of contract committed by the ***payment institution or its agents***;

   (c) ***relevant*** information ***or*** documents have ***not*** been received from the applicant for an account;

---

27 Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (Text with EEA relevance), OJ L, 2024/1624, 19.6.2024, p.1

▌

(ea) the competent authority has refused to grant or has withdrawn an authorisation as a payment institution.

▌

2. Rights granted under paragraph 1 to agents ▌ shall be granted exclusively for the provision of payment services on behalf of the payment institution.

3. ***Without undue delay and at the latest one month after receiving a complete application,*** a credit institution shall notify to the payment institution or to its agents or ▌ to the applicant for ***authorisation*** as a payment institution***, as well as to the competent authority***, any decision to refuse to open ▌ a payment account to a payment institution or to its agents ▌ or to an applicant for ***authorisation*** 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 ▌ , as assessed by the credit institution, ***based upon grounds referred to in paragraph 1*** and not be generic in nature.

The credit institution shall notify to the payment institution or to its agents, as well as to the competent authority, of the decision to close the payment account at least 4 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, and shall consider the payment institution's ability to comply with the safeguarding requirement as set out in Article 9 of Directive (EU) [PSD3].

By way of derogation from the first and second subparagraphs, credit institutions shall in the cases covered under paragraph 1, point (a):

- only notify to the payment institution, its agents or the applicant for authorisation as a payment institution that opening or maintaining a payment account would result in an infringement of Regulation (EU) 2024/1624 and shall not disclose any detail on the nature of that infringement;

- be entitled to close the payment account following a shorter notice period.

3a. ***The competent authority may publish aggregate data on payment account refusals and closures.***

4. A payment institution or its agents ▌ , or an applicant for ***authorisation*** as a payment institution 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.

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.

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.

Chapter 3

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 ***to Directive XXX [PSD3]***. 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.

Article 34

Contractual relations

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

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. Account servicing payment service providers ***shall*** put in place ***their dedicated interface within three months of obtaining their authorisation. The account servicing payment service provider shall provide the relevant technical documentation of the*** dedicated interface ***without undue delay, upon request by authorised*** payment initiation service providers***, account information service providers or by undertakings that have applied to their competent authorities for the relevant authorisation so that these service providers can use the dedicated interface as soon as possible***.
Account servicing payment service providers shall always permit access to the dedicated interface in order to allow business continuity for payment initiation service providers and account information service providers.

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, widely recognised standards offering equivalent security***. 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, ***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***, as a minimum through publication on their website,*** to authorised payment initiation service providers, account information service providers, or ▌ relevant ***applicant payment institutions as defined in Article 2(39b) of [PSD3]***, in advance, as soon as possible and not less than ***2*** 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***, 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 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 ▌ relevant ***applicant payment institutions as defined in Article 2(39b) of [PSD3]***, 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.

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 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;

(b) instruct the account servicing payment service provider to start the authentication based on the ***consent*** 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;

▌

3. Account servicing payment service providers shall allow account information service providers to communicate securely, via the dedicated interface, ***in order*** to request and receive information on one or more designated payment accounts and associated payment transactions. ***That information shall include the unique identifier of the account, the associated name of the account holder, the currencies, the account balance, and payment transactions initiated through a payment instrument which have not yet been charged to the payment account, if those transactions are already visible in the customer interface.***

4. Account servicing payment service providers shall ensure that the dedicated interface allows payment initiation service providers, at a minimum, to:

(a) place and revoke a standing payment order ▌ ;

(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***, unless the payment service user is unable to perform those payments in the customer interface***;

(f) communicate securely to place a payment order from the payer's payment 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;

[redacted]

(ha) in cases where the account servicing payment service provider offers multiple authentication procedures, choose which authentication procedure is to be presented to the payer;

[redacted]

(hc) prior to initiation of the payment, see the unique identifier of the account, the associated names of the account holder and the currencies, where available to the payment service user.

5. Account servicing payment service providers shall ensure that the dedicated 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 ***as soon as possible,*** that the payment ***has been or*** 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.

5a. ***For the purposes of the activities of payment initiation service providers and account information service providers, the name of the account owner and the unique identifier of the account 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 ***that is*** made available to the payment service user when directly requesting access to the account information, provided that this 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 ***as is*** 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***. Any update to that information, including to the payment status, shall be made available to the payment initiation service provider via the dedicated interface*** and on an ongoing basis until the payment is ***executed or rejected***.

▌

Article 38

***Availability and performance requirements for the* dedicated interface**

1. Account servicing payment service providers shall take all measures in their power to ***limit planned*** unavailability ***of the dedicated interface to the extent strictly necessary and to prevent unplanned unavailability and underperformance*** 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 ***server error responses or*** no response from the account servicing payment service provider's dedicated interface within 30 seconds.

2. In case of ***planned*** unavailability of the dedicated interface, account servicing payment service providers shall***, 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.***

2a. 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 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. Account servicing payment service providers shall ensure an optimal recovery time of the dedicated interface.

2b. The account servicing payment service providers shall ensure that the dedicated interface provides availability and performance that are equal at least to those of 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 the interfaces referred to in Article 35(5) 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.

For the purposes of point (b) of the first subparagraph, 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 [OP please insert the date = nine months 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.

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, ▌ the interfaces that the account servicing payment service provider uses for authentication and communication with its payment services users ***provided this interface offers equivalent functionality to support access by payment initiation service providers and account information service providers and uses widely accepted and interoperable standards*** or, where justified, not to offer any interface at all for secure data exchange. ***Where appropriate, Member States may exempt national central banks not acting in their capacity as monetary authority or other public authorities referred to in Article 2, paragraph 1, letter (d) of this Regulation, from the obligation to have in place a dedicated interface.***

2. The EBA shall develop draft regulatory technical standards which shall specify the criteria on the basis of which, in accordance with paragraph 1, ***it is justified for*** an account servicing payment service provider ▌ not to ***offer*** any interface at all for secure data exchange. ***When specifying those criteria, the EBA shall, inter alia, consider the size, annual turnover and payments volume of the account servicing payment service provider.***

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

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***, and on an ongoing basis, on request*** from a payment initiation service provider, ▌ 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;

(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.

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***, including any payment status update,*** about the execution of the payment order is made available to the payment initiation service provider immediately after that information becomes 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.

2. Account servicing payment service providers shall allow account information 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.

2a. Where the account information service provider intends to access information based on paragraph 2 at times when the payment service user is not actively requesting such information, it shall ensure that the payment service user is duly aware of that intention before making use of that 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 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 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 ***consents that*** 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***, at any time and in a format that is easy to understand,*** with an overview of each ongoing ***consent*** given for the purposes of account information services or payment initiation services, 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 ***consent***;

(iv) the period of validity of the ***consent, including the date on which the payment service user has given that consent***;

(v) the categories of data being shared***;***

(va) the dates on which payment account data was accessed.

(b) allow the payment service user to withdraw data access ***for all account information service or payment initiation service providers or*** for a given account information service or payment initiation service provider ***at any time and free of charge***;

(c) ***within 48 hours from withdrawal of a consent,*** allow the payment service user to re-establish any data access withdrawn;

▌

(d) include a record of data access ***consents*** that have been withdrawn or ***that*** have expired, for a duration of two years***;***

▌

2b. ***Where, pursuant to paragraph 2, point (b), a payment service user decides to withdraw data access, the payment initiation service provider or account information service provider concerned shall: - cease accessing and using the data; and - delete without undue delay, but not before 48 hours from withdrawal of a consent, the data received as a result of the data access consent granted by the payment services user. By way of derogation from the second indent of this paragraph, the payment service provider may retain the data if the payment service user explicitly so chooses.***

▌

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***.

The account servicing payment service provider shall not: - prompt the payment service user to withdraw a consent given for the purposes of account information services or payment initiation services; - design, organise or operate its dashboard in a manner that deceives, manipulates, or directs the payment service user to grant consents that are not in the user's best interest, or in a manner that materially distorts or impairs the user's ability to make free and informed decisions.

3b. The account information service or payment initiation service provider to which consent has been granted shall provide the information referred to in paragraph 2, point (a), to the account servicing payment service provider without undue delay. The account servicing payment service provider shall only provide the information referred to in paragraph 2, point (a), to the extent that it was provided to it by the account information service or payment initiation service provider to which consent has been granted.

4. The account servicing payment service provider and the account information service or payment initiation service provider to which ***consent*** has been granted shall cooperate to make information available to the payment service user via the dashboard ***without undue delay.***

The account servicing payment service provider shall ***make information available to*** the account information service or payment initiation service provider ***without undue delay of any*** changes made ***by the*** payment service user via the dashboard ***to a consent, including the withdrawal of a permission.***

An account information service or payment initiation service provider shall inform the account servicing payment service provider ***without undue delay*** of a new ***consent*** 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).***

4a. The account servicing payment service provider shall bear no liability for the actions referred to in 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.

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 ***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 service provider to be able to use account information or payment initiation services;

(c) requiring ▌ 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;

(e) requiring, unless ***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 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***, unless the payment service user is unable to perform those payments in the customer interface***;

(g) 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;

(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;

(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;

(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 ***the dedicated interface does not support all*** the authentication ***procedures made available by the*** account servicing payment service provider ***to its payment service users***;

(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.

1a. Measures taken by account servicing payment service providers which are necessary to address suspected fraud under this Regulation or to comply with Regulation (EU) 2016/679 shall not be deemed to constitute obstacles to data access unless those measures are prohibited obstacles referred to in points (a) to (l) of paragraph 1.

SECTION 4

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, ***other than*** in the circumstances covered by Article ***39 or exceptionally via another safe and efficient interface***.

2. Where ***only the interface referred to Article 39 is accessible to a payment initiation service provider or*** an 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 in accordance with Article 43(2), point (a), points (ii) to (v);

   (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 than for the provision of the service as requested by the payment service user;

(d) ***in order to allow the competent authority to investigate compliance with this Section,*** 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. ▌

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 ***to the extent that*** 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:

(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 ***consent*** , 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 ***consent***;

(f) every time a payment is initiated, identify itself towards the account servicing payment service provider and communicate with the account servicing payment service provider, the payer and the payee in a secure way***;***

(fa) be able to refuse to initiate a payment transaction for objectively justified reasons.

2. Payment initiation service providers shall not:

(a) ***without prejudice to Article 45(2), point (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

1. The account information service provider shall:

(a) provide services only where based on the payment service user's ***consent*** , 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 payment accounts and associated payment transactions, in accordance with the payment service user's ***consent***.

2. The account information service provider shall not:

(a) ***access*** sensitive payment data linked to the payment accounts;

(b) ***process*** any data for purposes other than for performing the account information service permitted by the payment service user ▌ .

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

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 ***Articles 35(1) and 38*** 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 ***undue*** delay the necessary ***and adequate*** enforcement measures and impose any appropriate sanction ▌ .

2. Competent authorities shall take without delay every necessary enforcement 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.

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.

6. Competent authorities shall, on their initiative, hold ▌ joint meetings with account servicing payment service providers, payment initiation service and account information service providers ***for the purposes of paragraph 6a.***

6a. Competent authorities 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 and 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 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.

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

CHAPTER 4

Authorisation of payment transactions

Article 49

Authorisation

1. A payment transaction or a series of payment transactions shall be authorised only if the payer has given its ***consent*** for the execution of the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the account servicing payment service provider, after the execution of the payment transaction.

1a. A payment transaction shall not be deemed to be authorised where the transaction was initiated or modified by a third party who is acting without the consent of the payment service user, including by using the personalised security credentials of the payment service user fraudulently obtained.

2. Access to a payment account for the purpose of account information services or payment initiation services by payment service providers shall be authorised only if the payment service user has given its ***consent*** to the account information services provider or, respectively, to the payment initiation service provider, to access the payment account and the relevant data in that account.

3. In the absence of ***consent*** , a payment transaction or access to a payment account by an account information service provider or a payment initiation service provider shall be considered to be unauthorised.

4. Account servicing payment service providers shall not verify the ***consent*** given by the payment service user to the account information service provider or payment initiation service provider.

5. The ***consent*** referred to in paragraphs 1 and 2 shall be expressed in the form agreed between the payer and the relevant payment service provider. ***Consent*** to execute a payment transaction may also be expressed via the payee or the payment initiation service provider.

6. The procedure for giving ***consent*** shall be agreed between the payer and the relevant payment service provider.

7. The payment service user may withdraw ***consent*** to execute a payment transaction or to access a payment account for the purpose of payment initiation services ***at any time, but no later than at the moment of irrevocability in accordance with Article 66. The payment service user may withdraw consent to access a payment account for the purpose of*** account information services ▌ at any time. The payment service user may also withdraw ***consent*** to execute a series of payment transactions, in which case any future payment transaction ***in that series*** shall be considered to be unauthorised.

Article 50

Discrepancies between the name and unique identifier of a payee in case of credit transfers

In the case of credit transfers, payment service providers shall comply with provisions of Articles 5c(1) to (7) and 5b(2) of Regulation (EU) 260/2012, and those articles shall apply mutatis mutandis to all credit transfers, including those that fall outside the scope of Regulation (EU) 260/2012.

For the purpose of the first subparagraph, where the payment account of the payee is not identified by the payment account identifier specified in point (1)(a) of the Annex of Regulation (EU) 260/2012, references in Article 5c of that Regulation to the payment account identifier shall be construed as referring to the unique identifier used to unambiguously identify the payment account of the payee.

Article 51

Limits and blocking of the use of the payment instrument

1. ***The*** payment service provider ***shall offer to the*** payment ***service user in the framework contract the possibility of setting in that contract a limit of a maximum amount that can be transferred, which may differ according to each means of payment, including for credit transfers, and each*** payment instrument. ***A limit may be on a per-transaction basis or within a set timeframe, at the sole discretion of the payment service user.***
Payment service providers shall not unilaterally ***change*** the spending limits ***set in the framework contract*** with their payment service users.
It shall be possible for the payment service user to modify the spending limits set in the framework contract. Payment service providers shall ensure that the payer is able to modify the spending limits set prior to the placing of a payment order.

1a. If the payment service user increases the spending limits remotely, payment service providers shall set a delay of four hours for that increase to come into effect. Payment service users shall have the right to adjust or opt out of the application of such delay period. Where a delay period is in place, any subsequent adjustment or opting out of its application shall be subject to the delay period in place.

Payment service providers shall immediately notify payment service users, in an agreed manner, when a change to a spending limit is requested, when the delay period referred to in the first subparagraph has ended or when the opt-out referred to in the first subparagraph is exercised.

1c. ***Where a payment service user's payment order exceeds, or leads to exceeding of the maximum amount, the payer's payment service provider shall not execute the payment order and shall inform the payment service user of the reasons thereof and how to modify the maximum amount.***

2. ▌The payment service provider may ▌ block the payment instrument for objectively justified reasons relating to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer ***might*** be unable to ***meet its obligation*** to pay.

3. In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the ***specific*** reasons for it in an agreed manner, where possible before the payment instrument is blocked and at the latest immediately thereafter, unless providing such information ▌ is prohibited by other relevant Union or national law. ***The payer's payment service provider shall without undue delay and within two business days at the latest, assess whether the reasons to block the payment instrument are still justified.***

4. The payment service provider shall unblock the payment instrument or replace it with a new payment instrument once the reasons for blocking no longer exist.

4a. Where the payment service provider offers the payment service user the possibility to initiate or give consent to payment transactions by means of a mobile application, the payment service provider shall require strong customer authentication and the use of different communication channels to activate the mobile application.

4b. If the payment service user activates the mobile application remotely, the provider shall set a delay of four hours for that activation to take effect. The payment service user shall have the right to adjust or opt out of the application of such a delay period. Where a delay period is in place, any subsequent adjustment or opting out of its application shall be subject to the delay period in place.

4c. The payment service provider shall immediately notify the payment service user, in an agreed manner, and through different communication channels, of the activation of a mobile application. The notification shall include instructions in case the payment service users have not installed the mobile application themselves.
The procedure for the notification referred to in this paragraph shall be agreed between the payment service user and the payment service provider.

4d. Where the payment service user notifies the payment service provider that they have not activated the mobile application linked to their payment account in accordance with the procedure referred to in paragraph 4c, the payment service provider shall without undue delay ensure that the mobile application does not make it possible to access the payment account of the payment service user, or initiate or give consent to payment transactions.

4e. Paragraphs 4a, 4b and 4c shall not apply to the initial establishment of the customer relationship between the payment service user and the payment service provider through the use of a mobile application nor to the activation by the payment service provider at its physical premises of a mobile application on a device of the payment service user.

4f. This Article applies to all credit transfers, including credit transfers in euro, notwithstanding Regulation (EU) 260/2012.

Article 52

Obligations of the payment service user in relation to payment instruments and personalised security credentials

The payment service user entitled to use a payment instrument shall:

(a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument, which shall be objective, non-discriminatory and proportionate;

(b) notify the payment service provider, or the entity specified by the payment service provider, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument ***or its relevant personalised security credentials***.

For the purposes of point (a) the payment service user shall, as soon as in receipt of a payment instrument, take all reasonable steps to keep its personalised security credentials safe.

Article 53

Obligations of the payment service provider in relation to payment instruments

1. The payment service provider issuing a payment instrument shall:

(a) ***ensure*** that the personalised security credentials are not accessible to parties other than the payment service user that is entitled to use the payment instrument, without prejudice to the obligations on the payment service user set out in Article 52;

(b) refrain from sending an unsolicited payment instrument, except where a payment instrument already given to the payment service user is to be replaced;

(c) ensure that appropriate means are available at all times ***and free of charge*** to enable the payment service user to make a notification pursuant to Article 52 point (b), or to request unblocking of the payment instrument pursuant to Article 51(4)***, and that human support is available free of charge for those purposes in an official language of the Member State where the payment service is provided at least during business hours***;

(d) provide the payment service user with the possibility to make a notification pursuant to Article 52 point (b) free of charge and only charge any possible replacement costs directly attributed to the payment instrument;

(e) prevent all use of the payment instrument once a notification pursuant to Article 52 point (b) has been made***;***

(ea) ensure that sensitive payment data are transmitted to the payment service user through safe channels.

For the purposes of point (c), the payment service provider shall provide the payment service user upon its request with the means to prove, for 18 months after notification, that the payment service user made such a notification.

2. The payment service provider shall bear the risk of sending a payment instrument or any personalised security credentials relating to it to the payment service user.

Article 54

Notification and rectification of unauthorised, authorised or incorrectly executed payment transactions

1. The payment service provider shall only rectify any unauthorised, incorrectly executed payment transaction or authorised payment transaction where the payment service user notifies the payment service provider in accordance with ***Article 56, 59 or 83*** without undue delay after becoming aware of any such transaction giving rise to a claim, including a claim under Article 75, and no later than ***18*** months after the debit date.

   The time limits for notification laid down in the first subparagraph shall not apply where the payment service provider has failed to provide or make available the information on the payment transaction in accordance with Title II.

2. Where a payment initiation service provider is involved, the payment service user shall obtain rectification from the account servicing payment service provider pursuant to paragraph 1 of this Article, without prejudice to Article 56(4) and Article 75(1).

Article 55

Evidence on authorisation and execution of payment transactions

1. Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the burden shall be on the payment service provider to prove that the payment transaction was authorised, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.

   If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authorised, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

2. Where a payment service user denies having authorised an executed payment transaction, ***the fact that*** the payment ***transaction was authenticated***, including ***where applicable, via strong customer authentication, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the*** service ***provided*** shall in itself not ***necessarily*** 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. The payment service provider, including, where appropriate, the payment initiation service provider, shall provide supporting evidence to prove fraud or gross negligence on part of the payment service user.

2a. For the purposes of paragraphs 1 and 2, and before concluding that a payment service user has authorised the transaction, acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52, the payment service provider shall invite the payment service user to provide information regarding the events leading up to the payment transaction and include this information in its assessment. Where the payment service user does not provide such information, this shall not in itself lead the payment service provider to conclude that the payment service user has authorised the transaction, acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52. The payment service user shall not be expected to provide information beyond what such a payment service user can reasonably be expected to have.

Article 56

Payment service provider's liability for unauthorised payment transactions

1. Without prejudice to Article 54, in the case of an unauthorised payment transaction, the payer's payment service provider shall refund the payer the amount of the unauthorised payment transaction immediately, and in any event no later than by the end of the following business day, after noting or being notified of the unauthorised transaction, except where the payer's payment service provider has ***objectively justified reasons for suspecting that the payer failed with intent or gross negligence to fulfil one or more of the obligations under Article 52, and communicates those*** grounds ***to the payer in writing, or*** for suspecting fraud committed by the payer ▌ .

2. Where the payer's payment service provider had ***objectively justified reasons*** for suspecting ***that*** the payer ***acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52***, the payer's payment service provider shall, within ***15*** business days after noting or being notified of the transaction, do either of the following:

   (a) refund the payer the amount of the unauthorised payment transaction if the payer's payment service provider has concluded, after further investigation, that ▌ the payer ***did not act fraudulently or fail with intent or gross negligence to fulfil one or more of the obligations under Article 52***;

(b) provide a justification ***to the payer*** for refusing the refund and indicate the bodies to which the payer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the payer does not accept the reasons provided***, and, where the payment service provider concludes that the payer acted fraudulently, communicate the reasons for that conclusion to the relevant national authority***.

For the purpose of the paragraph 2, point (b), Member States shall publish the name of the relevant national authority to whom the justification is to be provided.

3. Where applicable, the payer's payment service provider shall restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place. The payer's payment service provider shall also ensure that the credit value date for the payer's payment account shall be no later than the date the amount had been debited.

4. Where the payment transaction is initiated through a payment initiation service provider, the account servicing payment service provider shall refund immediately, and in any event no later than by the end of the following business day, the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

5. If the payment initiation service provider is liable for the unauthorised payment transaction, the payment initiation service provider shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer, including the amount of the unauthorised payment transaction. In accordance with Article 55(1), the burden shall be on the payment initiation service provider to prove that, within its sphere of competence, the payment transaction was authorised, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

6. ***Any*** further financial ***loss caused to the payer may be compensated*** in accordance with the law applicable to the contract concluded between the payer and the ***relevant*** payment service provider ▌ .

Article 57

Payment service provider's liability for incorrect application of the matching verification service

Where payment service providers fail to comply with Article 50, and where that failure results in a defectively executed payment transaction, the payer's payment service provider shall without delay refund the payer the amount transferred and, where applicable, restore the debited payment account to the state in which it would have been had the transaction not taken place.

Where that failure occurs because the payee's payment service provider, or the payment initiation service provider, failed to comply with Article 50, the payee's payment service provider or, where relevant, the payment initiation service provider, shall compensate the payer's payment service provider for the financial damage caused to the payer's payment service provider by that failure.

Any further financial loss caused to the payer may be compensated in accordance with the law applicable to the contract concluded between the payer and the relevant payment service provider.

Article 58

Liability of technical service providers and of operators of payment schemes for failure to support the application of strong customer authentication

Technical service providers and operators of payment schemes that either provide services to the payee, or to the payment service provider of the payee or of the payer, shall be liable for ***direct*** financial damage caused to the payee, to the payment service provider of the payee or of the payer for***, and proportionate to,*** their failure, within the remit of their contractual relationship, ***and not exceeding the amount of the transaction in question*** to provide the services that are necessary to enable the application of strong customer authentication.

Article 59

Payment service provider's liability for impersonation fraud

-1. Payment service providers shall have adequate prevention and robust technical safeguards in place to prevent cases where fraudsters replicate and misuse the payment service provider's communication channels for misleading payment service users into making fraudulent transactions.

1. Where a payment services user who is a consumer was manipulated by a third party pretending to be ▌ the consumer's payment service provider using ***communication channels attributed to the consumer's*** payment service provider ▌ and that manipulation gave rise to subsequent fraudulent authorised payment transactions, the payment service provider shall refund the consumer the full amount of the fraudulent authorised payment transaction under the condition that the consumer has, without ***undue*** delay ***after becoming aware of*** the fraud***,*** notified its payment service provider ***and reported the fraud to the police***.

2. Within ***15*** business days ***of*** being notified ***and provided with the police report by the consumer***, the payment service provider shall do either of the following:

(a) refund the consumer the amount of the fraudulent authorised payment transaction;

(b) where the payment service provider ***has objectively justified reasons*** to suspect a fraud or a gross negligence by the consumer, provide a justification for refusing the refund and indicate to the consumer the bodies to which the consumer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the consumer does not accept the reasons provided ***and, where the payment service provider concludes that the payer acted fraudulently, communicate the reasons for that conclusion to the national authority referred to in paragraph 56(2), point (b)***.

3. Paragraph 1 shall not apply if the consumer has acted fraudulently or with gross negligence.

4. The burden shall be on the payment service provider of the consumer to prove that the consumer acted fraudulently or with gross negligence.
Before concluding that the consumer acted fraudulently or with gross negligence, the payment service provider shall invite the consumer to provide information regarding the events leading up to the payment transaction and include this information in its assessment. Where the consumer does not provide such information, this shall not in itself lead the payment service provider to conclude that the consumer acted fraudulently or with gross negligence. The consumer shall not be expected to provide information beyond what such a consumer can reasonably be expected to have.

Article 59a

Cross-sectoral cooperation for the purpose of fraud prevention and detection

-1. ***Where payment fraud originates in the publication of fraudulent content online, payment service providers shall, without undue delay, inform providers of hosting services following the procedure laid down in Article 16, or, where applicable, Article 22 of Regulation (EU) 2022/2065.***

1. ***To the extent necessary for the purposes of preventing and detecting potentially fraudulent payment transactions, including transactions involving payment initiation services, data may be exchanged, when there are objectively justified grounds to suspect fraudulent behaviour by a user of their service:***

(a) between payment service providers and providers of hosting services, as defined in Article 3, point (g)(iii), of Regulation (EU) 2022/2065;

(b) between payment service providers and providers of electronic communications services, as defined in Article 2(4), point (b), of Directive (EU)2018/1972.

2. For the purpose of the first paragraph, without prejudice to Directive (EU) 2022/2555, Directive 2002/58/EC or Article 91 of this Regulation, providers of electronic communications services as defined in Article 2(4), point (b), of Directive (EU) 2018/1972 and providers of very large online platforms and of very large online search engines within the meaning of Article 33 of Regulation (EU)2022/2065 shall establish dedicated communication channels with payment service providers, or participate in a system for effective communication or in an information sharing mechanism, to allow for faster and more effective exchanges in compliance with Regulation (EU) 2016/679 and Directive 2002/58/EC.

3. Providers of electronic communications services as defined in Article 2(4), point (b), of Directive (EU) 2018/1972 and providers of very large online platforms and of very large online search engines within the meaning of Article 33 of Regulation (EU)2022/2065 shall have in place all necessary educational measures, including alerts to their recipients of their services via all appropriate means and media when new forms of online scams emerge, taking into account the needs of their most vulnerable groups of recipients of their services.

For the purpose of the first subparagraph, providers of electronic communication services as defined in Article 2(4), point (b), of Directive (EU) 2018/1972 shall give the recipients of their services clear indications as to:

(i) how to identify fraudulent attempts;

(ii) actions and precautions to be taken to avoid falling victim to fraudulent actions targeting them; and

(iii) the procedure for reporting fraudulent actions.

For the purpose of the first subparagraph, providers of very large online platforms and of very large online search engines within the meaning of Regulation (EU) 2022/2065 shall give the recipients of their services clear indications as to:

(i) how to identify fraudulent attempts;

(ii) actions and precautions to be taken to avoid falling victim to fraudulent actions targeting them; and

(iii) the procedure for reporting fraudulent actions, for the purpose of compliance with Article 16 of Regulation (EU) 2022/2065.

4. The Commission and the European Board of Digital Services shall encourage and facilitate the drawing up of a voluntary code of conduct at Union level to foster prevention, enhance security and combat payment fraud and financial scams, under the conditions set out in Article 45 of Regulation 2022/2065.

5. Without prejudice to Directive (EU) 2022/2555, electronic communications services providers as defined under Article 2(4), point (b) of Directive (EU) 2018/1972 shall take appropriate organisational and technical measures to detect and prevent the use of their services for impersonation fraud, including by means of manipulation of calling line identification or electronic mail address, where that use aims to induce payment services users to make a payment or to take an action that would compromise the security of the payment account. Those measures shall comply with applicable Union law, including Directive 2002/58/EC and Regulation (EU) 2016/679.

Article 59b

Advertising of regulated financial services on very large online platforms and very large online search engines

1. For the purposes of this Article, 'regulated financial service' means any service of a banking, credit, insurance, personal pension, payment or investment (including cryptoassets and crowdfunding) nature for which authorisation from or registration with a competent authority is required under Union law.

2. Providers of very large online platforms and of very large online search engines within the meaning of Article 33 of Regulation (EU)2022/2065, shall request from each advertiser of a regulated financial service an authorisation number, registration number or other information that that advertiser is a regulated financial service provider that is authorised or registered to provide the advertised regulated financial service in a Member State or at the Union level or is acting on behalf of such a provider.

2a. ***Providers of very large online platforms and of very large online search engines within the meaning of Article 33 of Regulation (EU) 2022/2065 shall, upon receiving the information referred to in paragraph 2, and prior to allowing the advertiser concerned to use their service for the purpose of advertising those regulated financial services, make best efforts, including by using the registers of authorised or registered providers of regulated financial services made available in accordance with Directive [PSD3] or other relevant Union law, to assess whether that information, for the accuracy of which advertisers are solely responsible for the purposes of this Regulation, is reliable and complete, provided that the assessment can be carried out in a proportionate manner by automated tools.***

3. ***Providers of very large online platforms and of very large online search engines within the meaning of Article 33 of Regulation (EU)2022/2065 who have not obtained the information referred to in paragraph 2 shall refuse to allow the advertiser of regulated financial services to use their service for the purpose of advertising those regulated financial services.***

4. For the purposes of compliance with Article 39(2), points (a), (b) and (c) of Regulation 2022/2065, where the subject matter of an advertisement is a regulated financial service, providers of very large online platforms and of very large online search engines within the meaning of Article 33 of Regulation (EU)2022/2065 shall include in their advertisement repositories information that the subject matter of the advertisement is a regulated financial service and whether the advertiser is acting on behalf of the regulated financial service provider referred to in paragraph 1.

Article 60

Payer's liability for unauthorised payment transactions

1. By way of derogation from Article 56, the payer may be obliged to bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 50, resulting from the ***loss, theft or*** misappropriation of a payment instrument ***or personalised security credentials***.

The first subparagraph shall not apply where any of the following occurred:

(a) the loss, theft or misappropriation of a payment instrument ***or personalised security credentials*** was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or

(b) the loss was caused by acts or lack of action of an employee, agent or branch of a payment service provider or of an entity to which its activities were outsourced.

[redacted]

Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 52, national competent authorities***, dispute resolution bodies*** or payment service providers may reduce the liability referred to in this paragraph, taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.

1a. The payer shall bear all of the losses relating to any unauthorised payment transactions if those losses were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations set out in Article 52 with intent or gross negligence. In such cases, the maximum amount referred to in the first paragraph shall not apply.

2. Where the payer's payment service provider fails to fulfil the obligation to require strong customer authentication set out in Article 85, the payer shall not bear any financial losses unless the payer has acted fraudulently. The ***payer*** shall ***not bear any financial losses also*** where either the payment service provider of the payer or of the payee applies an exemption from the application of strong customer authentication. Where the payee or the payment service provider of the payee fails to develop or amend the systems, hardware and software that are necessary to apply strong customer authentication, the payee or the payment service provider of the payee shall refund the financial damage caused to the payer's payment service provider.

3. Where the payee's payment services provider applies an exemption from the application of strong customer authentication, the payee's payment services provider shall be liable towards the payer's payment services provider for any financial loss incurred by the latter.

4. The payer shall not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification in accordance with of Article 52, point (b), except where the payer has acted fraudulently.

If the payment service provider does not provide appropriate means for the notification at all times of a lost, stolen or misappropriated payment instrument, as required under of Article 53(1), point (c), the payer shall not be liable for the financial consequences resulting from use of that payment instrument, except where the payer has acted fraudulently.

5. The Commission may adopt a delegated act in accordance with Article 106 to amend this Regulation by updating the amount referred to in paragraph 1.

Article 61

Payment transactions where the transaction amount is not known in advance

1. Where a payment transaction is initiated by or through the payee***, in particular*** in the context of a card-based payment ***or of a credit transfer,*** and the exact future amount is not known at the moment when the payer ***authorises*** the execution of the payment transaction, the payer's payment service provider may only block funds on the payer's payment account if the payer has given his or her ***consent*** to that precise amount of funds to be blocked.

2. The amount of the funds blocked by the payer's payment service provider shall be in proportion with the amount of the payment transaction which can reasonably be expected by the payer.

3. The payee shall inform its payment service provider of the exact amount of the payment transaction immediately after delivery of the service or goods to the payer.

4. The payer's payment service provider shall release the funds blocked on the payer's payment account immediately after receipt of the information about the exact amount of the payment transaction.

Article 62

Refunds for payment transactions initiated by or through a payee

1. A payer shall be entitled to a refund from the payment service provider of an authorised payment transaction which was initiated by ***or*** through a payee and which has already been executed, where both of the following conditions are met:

   (a) the authorisation did not specify the exact amount of the payment transaction when the authorisation was made;

   (b) the amount of the payment transaction exceeded the amount the payer could reasonably have expected taking into account the previous spending pattern, the conditions in the framework contract and relevant circumstances of the case.

   At the payment service provider's request, the payer shall bear the burden of proving such conditions are met.

The refund shall consist of the full amount of the executed payment transaction. The credit value date for the payer's payment account shall be no later than the date the amount was debited.

Without prejudice to paragraph 3 of this Article, in addition to the right referred to in the first subparagraph of this paragraph, for ▌ direct debits ▌ , the payer shall have an unconditional right to a refund within the time limits laid down in Article 63 of this Regulation.

2. For the purposes of paragraph 1, first subparagraph, point (b), the payer shall not invoke reasons related to possible currency exchange costs if the reference exchange rate agreed with its payment service provider in accordance with Article 13(1), point (e), and Article 20, point (c)(iii), was applied.

3. The payer and the payment service provider may agree in a framework contract that the payer has no right to a refund where:

(a) the payer has authorised the execution of the payment transaction directly with the payment service provider;

(b) where applicable, information on the future payment transaction was provided or made available in an agreed manner to the payer for at least 4 weeks before the due date by the payment service provider or by the payee.

4. For direct debits in currencies other than euro, payment service providers may offer more favourable refund rights in accordance with their direct debit schemes provided that they are more advantageous to the payer.

Article 63

Requests for refunds for payment transactions initiated by or through a payee

1. The payer may request the refund referred to in Article 62 of an authorised payment transaction initiated by or through a payee for a period of 8 weeks from the date on which the funds were debited.

2. Within ***15*** business days of receiving a request for a refund, the payment service provider shall do either of the following:

   (a) refund the full amount of the payment transaction;

   (b) provide a justification for refusing the refund and indicate the bodies to which the payer may refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the payer does not accept the reasons provided.

   The payment service provider's right under the first subparagraph of this paragraph to refuse the refund shall not apply in the case set out in of Article 62(1), fourth subparagraph.

CHAPTER 5

Execution of payment transactions

SECTION 1

PAYMENT ORDERS AND AMOUNTS TRANSFERRED

Article 64

Receipt of payment orders

1. The time of receipt of a payment order shall be when the payment order is received by the payer's payment service provider.

   The payer's account shall not be debited before receipt of the payment order. If the time of receipt is not on a business day for the payer's payment service provider, the payment order shall be deemed to have been received on the following business day. The payment service provider may establish a cut-off time near the end of a business day beyond which any payment order received shall be deemed to have been received on the following business day.

2. If the payment service user placing a payment order and the payment service provider agree that the execution of the payment order shall start on a specific day or at the end of a certain period or on the day on which the payer has put the funds at the payment service provider's disposal, the time of receipt for the purposes of Article 69 shall be deemed to be the agreed day. If the agreed day is not a business day for the payment service provider, the payment order received shall be deemed to have been received on the following business day.

3. This Article shall not apply to instant credit transfers denominated in Euro as covered by Regulation XXX (IPR).

Article 65

Refusal *to execute a* payment *order*

-1. Where all of the conditions set out in the payer's framework contract are met, the payer's payment service provider shall not refuse to execute an authorised payment transaction, irrespective of whether the payment order is placed by a payer, including through a payment initiation service provider, or by or through a payee, unless relevant Union or national law provides otherwise.

-1a. By way of derogation from paragraph -1 and without prejudice to Regulation (EU) 2024/1624, the payer's payment service provider shall refuse to execute a payment transaction if the conditions set out in this Article are fulfilled.

Notwithstanding Article 5c(5) of Regulation (EU) No 260/2012 and Articles 50 and 69(1) of this Regulation, where, based on the transaction monitoring referred to in Article 83 of this Regulation or on any other relevant information available to the payment service provider, but not solely on the basis of the outcome of the service ensuring the verification of payee, the payer's payment service provider has objectively justified reasons to suspect that the transaction is fraudulent, the payer's payment service provider shall suspend the execution of a payment transaction.

Where the payer's payment service provider has objectively justified reasons to suspect that the transaction is fraudulent and does not suspend that transaction in accordance with the first subparagraph, the payer shall not bear any financial losses, except if the payer has acted fraudulently.

The burden of proof that there was no breach of this Article shall be on the payment service provider.

Without undue delay from the suspension of the transaction, unless prohibited by other relevant Union or national law, the payment service provider shall notify the payer, in an agreed manner, of any information or action needed from the payer to enable the payment service provider to assess, whether the reasons for such suspension are still justified. The notification shall give the payer sufficient information to enable the payer to understand the risks that the payment service provider has identified. Within the timelines specified in Article 69(1), the payment service provider shall make all reasonable efforts to contact the payer, and shall ensure that appropriate means are available at all times to enable the payer to contact the payment service provider where additional information is requested by the payment service provider to assess whether there are objectively justified reasons to suspect fraud.

On the basis of that assessment, the payer's payment service provider shall decide whether or not to execute the payment order and, where applicable, restore the debited payment account to the state in which it would have been had the payment order not been submitted.

The obligation to notify the payer under the fifth subparagraph shall not apply in the case of instant credit transfers. In such cases or where it has not been possible for the payer's payment service provider to receive information from the payer within the timelines specified in Article 69(1), the payment service provider shall assess, based on the transaction monitoring referred to in paragraph -1, and on any other relevant information available to the payment service provider, but not solely on the basis of the outcome of the service ensuring the verification of payee, whether or not to execute the payment order.

For the purpose of this Regulation, the fact that a payment order is unusual shall not by itself constitute objectively justified reasons to suspect fraud.

1. Where***, on the basis of the assessment in paragraph -1a,*** the payment service provider refuses to execute a payment order or to initiate a payment transaction, the ***payer's*** payment service provider shall notify ***to the payer and the payee's payment service provider and, where applicable, make available to the payment initiation service provider,*** the refusal ▌ , the ***specific*** reasons for that refusal and***, where applicable,*** the procedure for correcting ***the decision to refuse to execute the transaction***, unless ***such notification is*** prohibited ***under*** relevant Union or national law.

The ***payer's*** payment service provider shall ***make*** the notification in an agreed manner***, and where applicable shall make the information available to the payment initiation service provider, without undue delay***, and in any case within the periods specified in Article 69. ***In the case of instant credit transfers, the payer's payment service provider shall provide the notification, and where applicable shall make the information available to the payment initiation service provider, within 10 seconds of the time of receipt of the payment order by the payer's payment service provider.***

The framework contract may include a condition that the payment service provider may charge a reasonable fee for such a refusal if the refusal is objectively justified***, but not in the case of a refusal due to a suspected fraudulent transaction***.

3. For the purposes of Articles 69 and 75 a payment order whose execution has been refused shall be deemed not to have been received.

Article 66

Irrevocability of a payment order

1. The payment service user shall not revoke a payment order once it has been received by the payer's payment service provider, unless otherwise specified in this Article.

2. Where the payment transaction is initiated by a payment initiation service provider or by or through the payee, the payer shall not revoke the payment order after giving permission to the payment initiation service provider to initiate the payment transaction or after giving permission to execute the payment transaction to the payee.

3. In the case of a direct debit, and without prejudice to refund rights, the payer may revoke the payment order at the latest by the end of the business day preceding the day agreed for debiting the funds.

4. In the case referred to in Article 64(2), the payment service user may revoke a payment order at the latest by the end of the business day preceding the agreed day.

5. After the time limits laid down in paragraphs 1 to 4, the payment order may be revoked only if agreed between the payment service user and the relevant payment service providers. In the case referred to in paragraphs 2 and 3, the payee's agreement shall also be required. If agreed in the framework contract, the relevant payment service provider may charge for revocation.

Article 67

Amounts transferred and amounts received

1. The payment service provider of the payer, the payment service provider(s) of the payee and any intermediaries of the payment service providers shall transfer the full amount of the payment transaction and shall refrain from deducting charges from the amount transferred.

2. The payee and the payment service provider may agree that the relevant payment service provider deduct its charges from the amount transferred before crediting it to the payee. In such a case, the full amount of the payment transaction and charges shall be separated in the information given to the payee.

3. If any charges other than those referred to in paragraph 2 are deducted from the amount transferred, the payment service provider of the payer shall ensure that the payee receives the full amount of the payment transaction initiated by the payer. Where the payment transaction is initiated by or through the payee, the payment service provider of the payee shall ensure that the full amount of the payment transaction is received by the payee.

Article 67a

Payment transactions with electronic money tokens

1. By way of derogation from Article 13, points (b) and (d), Article 20, points (b)(v) and (c)(i) and Article 24 of this Regulation, where payment service providers are not able, due to circumstances that are not attributable to them, to comply with the obligations set out therein as regards payment transactions with electronic money tokens settled on the distributed ledger, the payment service providers shall provide the information required therein by way of a reasoned estimation, as soon as possible, and in any case prior to the payer authorising the transaction.

2. The requirements in Articles 40 and 41 of this Regulation for account servicing payment service providers regarding payment initiation services and account information services, shall not apply as regards payment transactions with electronic money tokens.

3. Articles 50 and 57 of this Regulation shall not apply to payment service providers as regards payment transactions with electronic money tokens.

4. The Commission may adopt delegated acts in accordance with Article 106 to amend this Regulation by adjusting the derogations and requirements set out in paragraphs 1, 2 and 3 of this Article as regards payment transactions with electronic money tokens to take into account developments after the adoption of this Regulation and the specificities of the use of distributed ledger technology or similar technology for such transactions.

SECTION 2

EXECUTION TIME AND VALUE DATE

Article 68

Scope

1. This Section applies to:

   (a) payment transactions in euro;

   (b) national payment transactions in the currency of the Member State outside the euro area;

   (c) payment transactions involving only one currency conversion between the euro and the currency of a Member State outside the euro area, provided that the required currency conversion is carried out in the Member State outside the euro area concerned and, in the case of cross-border payment transactions, the cross-border transfer takes place in euro.

2. This Section applies to payment transactions not referred to in paragraph 1, unless otherwise agreed between the payment service user and the payment service provider, with the exception of Article 73, which is not at the disposal of the parties. However, if the payment service user and the payment service provider agree on a longer period than that set in Article 69, for intra-Union payment transactions, that longer period shall not exceed ***5*** business days following the time of receipt as referred to in Article 64.

Article 69

Payment transactions to a payment account

1. Without prejudice to ***relevant Union or national legislation in the field of anti-money laundering and anti-terrorism financing***, the payer's payment service provider shall ensure that after the time of receipt as referred to in Article 64, the amount of the payment transaction will be credited to the payee's payment service provider's account by the end of the following business day. That time limit may be extended by a further business day for paper-initiated payment transactions.

▌

2. ***Without prejudice to relevant Union or national legislation in the field of anti-money laundering and anti-terrorism financing,*** the payment service provider of the payee shall value date and make available the amount of the payment transaction to the payee's payment account after the payment service provider has received the funds in accordance with Article 73.

2a. ***By way of derogation from paragraph 2, if, based on the transaction monitoring conducted in accordance with Article 83, or on any relevant information available to the payee's payment service provider, but not solely on the outcome of the service ensuring the verification of payee, the payee's payment service provider has objectively justified reasons to suspect that a payment transaction credited or to be credited to its account is fraudulent, that payment service provider may, in compliance with its obligations to refrain from carrying out suspicious transactions under Article 71 of Regulation (EU) 2024/1624, decide to not make the funds available on the payee's payment account and to return the funds to the payment service provider of the payer, provided that that decision takes place within the timeline set out in Article 73 of this Regulation.***

Where the reasons to suspect that a payment transaction credited or to be credited to the payee's account is fraudulent are clear and incontrovertible, the payee's payment service provider shall not make the funds available on the payee's payment account and shall return the funds to the payment service provider of the payer.

Where a payment service provider does not comply with the obligation set out in subparagraph 2, the payer shall not bear any financial losses, except if the payer has acted fraudulently.

The first and second subparagraphs shall be without prejudice to the obligation of the payee's payment service provider to report suspicious transactions set out in Article 69 of Regulation (EU) 2024/1624.

For the purpose of this Regulation, the fact that a payment order is unusual shall not by itself constitute objectively justified reasons to suspect fraud.

The burden of proof that there was no breach of subparagraph 2 shall be on the payment service provider of the payee.

2b. Where the payment service provider of the payee returns the funds to the payer's payment service provider pursuant to the first or second subparagraphs of paragraph 2a, the payment service provider of the payee shall:

(i) immediately notify the payment service provider of the payer of the return of the funds, and of the reasons for the refusal to make the funds available on the payee's payment account, in accordance with the rules on prohibition of disclosure set out in Article 73(5) of Regulation (EU) 2024/1624; and

(ii) ensure that the amount of the payment transaction is credited to the payer's payment service provider within the timeline set out in paragraph 1.

2c. Upon receiving the notification pursuant to paragraph 2b, point (i), the payment service provider of the payer shall, immediately and free of charge, inform the payer, and, where applicable, make the information available to the payment initiation service provider, that the funds have not been made available on the payee's payment account due to measures aimed at fraud prevention, without prejudice to Article 73 of Regulation (EU) 2024/1624. The payment service provider of the payer shall also inform the payer of the return of the funds and the timeline for making the amount of the payment transaction available on the payer's payment account. The payment service provider of the payer shall value date and make available the amount of the payment transaction credited to its account pursuant to paragraph 2b, point (ii), to the payer's payment account in accordance with Article 73 of this Regulation.

2d. In the case of instant credit transfers, where the payment service provider of the payee returns the funds to the payer's payment service provider pursuant to the first or second subparagraphs of paragraph 2a, the payment service provider of the payee shall:

(i) within 10 seconds of the time of receipt of the payment order for an instant credit transfer by the payer's payment service provider, notify the payer's payment service provider of the return of the funds, and of the reasons for the refusal to make the funds available on the payee's payment account, in accordance with the rules on prohibition of disclosure set out in Article 73(5) of Regulation (EU) 2024/1624; and

(ii) where the amount of the transaction has been credited to its account, ensure that those funds are credited immediately to the payer's payment service provider.

(iii)

2e. ***Immediately upon receiving the notification referred to in paragraph 2d, point (i), the payment service provider of the payer shall:***

(i) ***restore the payment account of the payer to the state in which it would have been had the transaction not taken place; and***

(ii) ***free of charge, inform the payer, and, where applicable, make the information available to the payment initiation service provider, of the return of the funds, and, without prejudice to Article 73 of Regulation (EU) 2024/1624, that the funds have not been made available on the payee's payment account due to measures aimed at fraud prevention.***

3. The payee's payment service provider shall transmit a payment order placed by or through the payee to the payer's payment service provider within the time limits agreed between the payee and the payment service provider, enabling settlement [redacted] on the agreed due date. ***Paragraph 2a shall apply accordingly.***

Article 70

Absence of payee's payment account with the payment service provider

Where the payee does not have a payment account with the payment service provider, the payment service provider who receives the funds for the payee shall make the funds available to the payee within the time limit laid down in Article 69(1).

In the case of payment transactions with electronic money tokens from a custodial wallet to a self-hosted address, the payment service provider of the payer shall transfer the funds to the self-hosted address of the payee within the time limit laid down in Article 69(1).

Article 71

Cash placed on a payment account

Where a consumer places cash on a payment account with that payment service provider in the currency of that payment account, the payment service provider shall ensure that the amount is made available and value dated immediately after receipt of the funds. Where the payment service user is not a consumer, the amount shall be made available and value dated at the latest on the following business day after receipt of the funds.

Article 72

National payment transactions

For national payment transactions, Member States may provide for shorter maximum execution times than those provided for in this Section.

Member States shall notify to the Commission the provisions of their law adopted pursuant to this Article. They shall, without delay, notify any subsequent amendments to such provisions.

Article 73

Value date and availability of funds

1. The credit value date for the payee's payment account shall be no later than the business day on which the amount of the payment transaction is credited to the payee's payment service provider's account.

2. The payment service provider of the payee shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account where, on the part of the payee's payment service provider, there is either of the following:

(a) no currency conversion;

(b) a currency conversion between the euro and a Member State currency or between two Member State currencies.

The obligation laid down in this paragraph shall also apply to payments within one payment service provider.

3. The debit value date for the payer's payment account shall be no earlier than the time at which the amount of the payment transaction is debited to that payment account.

Article 74

Incorrect unique identifiers

1. If a payment transaction is executed in accordance with the unique identifier, the payment transaction shall be deemed to have been executed correctly with regard to the payee specified by the unique identifier.

2. If the unique identifier provided by the payment service user is incorrect, the payment service provider shall not be liable under Article 75 for non-execution or defective execution of the payment transaction.

3. The payer's payment service provider shall make reasonable efforts to recover the funds involved in the payment transaction. The payee's payment service provider shall cooperate in those efforts also by communicating to the payer's payment service provider all relevant information for the collection of funds.

   Where the collection of funds under the first subparagraph is not possible, the payer's payment service provider shall provide to the payer, upon written request, all information available to the payer's payment service provider and relevant to the payer in order for the payer to file a legal claim to recover the funds.

4. Where agreed in the framework contract, the payment service provider may charge the payment service user for recovery. ***The charge shall be reasonable and proportionate to the costs incurred.***

5. If the payment service user provides information in addition to the information referred to in Article 13(1), point (a), or Article 20 point (b) (ii), the payment service provider shall be liable only for the execution of payment transactions in accordance with the unique identifier provided by the payment service user.

6. Where the unique identifier provided by the payment initiation service provider is incorrect, payment service providers shall be liable in accordance with Article 76.

Article 75

Payment service providers' liability for non-execution, defective or late execution of payment transactions

1. Where a payment order is placed directly by the payer, the payer's payment service provider shall, without prejudice to Article 54, Article 74(2) and (3), and Article 79, be liable to the payer for correct execution of the payment transaction, unless it can prove to the payer and, where relevant, to the payee's payment service provider that the payee's payment service provider received the amount of the payment transaction in accordance with Article 69(1). In that case, the payee's payment service provider shall be liable to the payee for the correct execution of the payment transaction.

Where the payer's payment service provider is liable under the first subparagraph, it shall immediately refund to the payer the amount of the non-executed or defective payment transaction, and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.

The credit value date for the payer's payment account shall be no later than the date on which the amount was debited.

Where the payee's payment service provider is liable under the first subparagraph, it shall immediately place the amount of the payment transaction at the payee's disposal and, where applicable, credit the corresponding amount to the payee's payment account.

The credit value date for the payee's payment account shall be no later than the date on which the amount would have been value dated, had the transaction been correctly executed in accordance with Article 73.

Where a payment transaction is executed late, the payee's payment service provider shall ensure, upon the request of the payer's payment service provider acting on behalf of the payer, that the credit value date for the payee's payment account is no later than the date the amount would have been value dated had the transaction been correctly executed.

In the case of a non-executed or defectively executed payment transaction where the payment order is placed by the payer, the payer's payment service provider shall, regardless of liability under this paragraph, on request and without charging the payer, make immediate efforts to trace the payment transaction and notify the payer of the outcome.

2. Where a payment order is placed by or through the payee, the payee's payment service provider shall, without prejudice to Article 54, Article 74(2) and (3), and Article 79, be liable to the payee for correct transmission of the payment order to the payment service provider of the payer in accordance with Article 69(3). Where the payee's payment service provider is liable under this subparagraph, it shall immediately re-transmit the payment order in question to the payment service provider of the payer.

In the case of a late transmission of the payment order, the amount shall be value dated on the payee's payment account no later than the date the amount would have been value dated had the transaction been correctly executed.

Without prejudice to Article 54, Article 74(2) and (3), and Article 79, the payment service provider of the payee shall be liable to the payee for handling the payment transaction in accordance with its obligations under Article 73. Where the payee's payment service provider is liable under this subparagraph, it shall ensure that the amount of the payment transaction is at the payee's disposal immediately after that amount is credited to the payee's payment service provider's account. The amount shall be value dated on the payee's payment account no later than the date the amount would have been value dated had the transaction been correctly executed.

In the case of a non-executed or defectively executed payment transaction for which the payee's payment service provider is not liable under the first and third subparagraphs, the payer's payment service provider shall be liable to the payer. Where the payer's payment service provider is so liable it shall, as appropriate and without undue delay, refund to the payer the amount of the non-executed or defective payment transaction and restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place. The credit value date for the payer's payment account shall be no later than the date the amount was debited.

The obligation under the fourth subparagraph shall not apply to the payer's payment service provider where the payer's payment service provider proves that the payee's payment service provider has received the amount of the payment transaction, even if execution of payment transaction is merely delayed. If so, the payee's payment service provider shall value date the amount on the payee's payment account no later than the date the amount would have been value dated had it been executed correctly.

In the case of a non-executed or defectively executed payment transaction where the payment order is placed by or through the payee, the payee's payment service provider shall, regardless of liability under this paragraph, on request and without charging the payer, make immediate efforts to trace the payment transaction and notify the payee of the outcome.

3. Payment service providers shall be liable to their respective payment service users for any charges for which they are responsible, and for any interest to which the payment service user is subject as a consequence of non-execution or defective, including late, execution of the payment transaction.

Article 76

Liability in the case of payment initiation services for non-execution, defective or late execution of payment transactions

1. Where a payment order is placed by the payer or by the payee through a payment initiation service provider, the account servicing payment service provider shall, without prejudice to Article 54 and Article 74(2) and (3), refund to the payer the amount of the non-executed or defective payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the defective payment transaction not taken place.

   The burden shall be on the payment initiation service provider to prove that the payment order was received by the payer's account servicing payment service provider in accordance with Article 64 and that within its sphere of competence the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the non-execution, defective or late execution of the transaction.

2. If the payment initiation service provider is liable for the non-execution, defective or late execution of the payment transaction, it shall immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer.

Article 77

Additional financial compensation

Any financial compensation additional to that provided for under this Section may be determined in accordance with the law applicable to the contract concluded between the payment service user and the payment service provider.

Article 78

Right of recourse

1. Where the liability of a payment service provider under Articles 56, 57, 59, 75***, 76 and 83*** is attributable to another payment service provider or to an intermediary, that payment service provider or intermediary shall compensate the first payment service provider for any losses incurred or sums paid under Articles 56, 57, 59, 75***, 76 and 83***. That shall include compensation where any of the payment service providers fail to apply strong customer authentication.

1a. Where a provider of hosting services within the meaning of Article 3(g)(iii) of Regulation (EU) 2022/2065 does not meet the conditions set out in Article 6(1), points (a) and (b), of that Regulation, in respect of the storage of illegal content within the meaning of Article 3(h) of that Regulation and where such content gives rise to one or a series of unauthorised payment transactions as referred to in Article 56, or to one or a series of fraudulent authorised payment transactions as referred to in Article 59, that provider shall compensate the payment service provider for any losses incurred or sums paid under Articles 56 and 59.

2. Further financial compensation may be determined in accordance with agreements between payment service providers or intermediaries and the law applicable to the agreement concluded between them.

Article 79

Abnormal and unforeseeable circumstances

No liability shall arise under Chapter 4 or 5 in cases of abnormal and unforeseeable circumstances beyond the control of the party pleading for the application of those circumstances, the consequences of which would have been unavoidable despite all efforts to the contrary, or where a payment service provider is bound by other legal obligations covered by Union or national law.

CHAPTER 6

Data protection

Article 80

Data protection

Payment systems***, payment schemes, processing entities*** and payment service providers shall be allowed to process special categories of personal data as referred to in Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725 to the extent necessary for the provision of payment services and for compliance with obligations under this Regulation, in the public interest of the well-functioning of the internal market for payment services, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, including the following:

(a) technical measures to ensure compliance with the principles of purpose limitation, data minimisation and storage limitation, as laid down in Regulation (EU) 2016/679, including technical limitations on the re-use of data and use of state-of-the-art security and privacy-preserving measures, including pseudonymisation, or encryption;

(b) ***organisational*** measures, including training on processing special categories of data, limiting access to special categories of data and recording such access.

CHAPTER 7

Operational and security risks and authentication

Article 81

Management of operational and security risks

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

   The first subparagraph shall be without prejudice to the application of Chapter II of Regulation (EU) 2022/2554 of the European Parliament and of the Council[28] to:

   (a) payment service providers referred to in Article 2(1), points (a), (b) and (d) of this Regulation;

[28] 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).

(b) account information service providers referred to in Article 36(1) of Directive (EU) (PSD3); and

(c) payment institutions exempted pursuant to Article 34(1) of Directive (EU) (PSD3).

[redacted]

2. The EBA shall promote cooperation, including the sharing of information, in the area of operational and security risks associated with payment services among the competent authorities, between the competent authorities and the ECB and, where relevant, the European Union Agency for Network and Information Security.

Article 82

Fraud reporting

1. Payment service providers shall provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide the EBA and the ECB with such data in an aggregated form.

Statistical data on fraud shall include the number and value of refunded fraudulent transactions and of transactions where refund has been refused in accordance with this Regulation, together with the reason for that refusal, such as stating that the consumer has acted fraudulently or with gross negligence.

1a. ***Competent authorities may allow payment service providers to fulfill the obligation in paragraph 1 by reporting fraud data under another data reporting requirement, if that requirement is not less extensive than the reporting requirement under this Article and if arrangements have been made under which the EBA and the ECB will receive the data that is due under this Article.***

1b. ***The EBA and the ECB shall publish in an annual joint report the statistical data in aggregated form and an analysis of the trends observed on the basis of those data.***

2. The EBA shall, in close cooperation with the ECB, develop draft regulatory technical standards on statistical data to be provided in accordance with paragraph 1 on the fraud reporting requirements referred to in paragraph 1.

The EBA shall submit the regulatory technical standards referred to in 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 regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

3. The EBA shall develop draft implementing technical standards establishing the standard forms and templates for the submission of the payment fraud data by competent authorities to the EBA, as referred to in paragraph 1. ***These implementing technical standards shall not be applicable if the competent authority makes use of the option referred to in paragraph 1a.***

The EBA shall submit the implementing technical standards referred to in 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 ***implementing*** technical standards referred to in the first subparagraph in accordance with Article 15 of Regulation (EU) No 1093/2010.

Article 83

Transaction monitoring mechanisms ▌

1. Payment service providers shall have transaction monitoring mechanisms in place ***to***:

   (a) support the application of strong customer authentication in accordance with Article 85;

   (b) exempt the application of strong customer authentication based on the criteria under Article 85(11), subject to specified and limited conditions based on the level of risk involved, the types and details of the data assessed by the payment service provider;

   (c) ▌ prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services.

1a. The payment service provider of the payer shall carry out the transaction monitoring referred to in paragraph 1 prior to the execution of a payment transaction. The payment service provider of the payee shall also carry out transaction monitoring before the funds are made available to the payee in accordance with Article 69(2).

Where a payment service provider does not carry out such monitoring with respect to a transaction and the payer incurs financial damage, that payment service provider shall bear liability.

Where the payer's payment service provider does not provide evidence to the payer that such monitoring for a transaction has been carried out by both providers, it shall refund the payer the amount of the transaction.

The payer shall not bear any financial consequences from that transaction, except where the payer has acted fraudulently.

The burden to prove that there was no breach of this Article shall be on the payment service provider concerned.

1b. Transaction monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts online.

2. Processing ***by the payment service provider of the payer*** shall be limited to the following data***, insofar as necessary to achieve*** the purposes referred to in paragraph 1:

(a) information on the ***payer***, including the environmental and behavioural characteristics which are typical of the ***payer*** in the circumstances of a normal use of the personalised security credentials;

(b) information on the payment account, including the payment transaction history;

(c) transaction information, including the transaction amount***, payment instrument, currency, date and time of execution, as well as*** unique identifier of the payee;

(d) session data, including the device internet protocol address-range from which the payment account has been accessed***, from which the transaction was initiated;***

(e) device data, including device identifiers from which the transaction was initiated;

(ea) information on the payee, including the unique identifier of the payee;

(eb) information received through the information sharing arrangements.

2a. Processing by the payment service provider of the payee shall be limited to the following data, insofar as necessary to achieve the purpose referred to in paragraph 1, as applicable:

(a) information on the payee;

(aa) information received through the information sharing arrangements;

(b) information on the payment account of the payee, including the payment transaction history;

(c) transaction information, including the transaction amount, payment instrument, currency, date and time of execution, as well as the name of the payer.

▌

2b. Payment service providers shall not store data referred to in ***paragraphs 2 and 2a*** longer than necessary for the purposes set out in paragraph 1, and***, in any event, no longer than 5 years*** after the termination of the customer relationship. ▌

Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:

(a) lists of compromised or stolen authentication elements;

(b) the amount of each payment transaction;

(c) known fraud scenarios in the provision of payment services;

(d) signs of malware infection in any sessions of the authentication procedure;

(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

Article 83a

Fraud information sharing

1. Payment service providers shall participate in information sharing arrangements with other payment service providers as referred to in paragraph 3 and shall exchange data to the extent necessary to comply with their obligations in Article 83(1), point (c), where the payment service provider has objectively justified reasons to suspect fraudulent behaviour by a payment service user. The categories of data to be shared shall be limited to the data listed in Article 83(2), points (a) to (ea), and 83(2a), points (a), (b) and (c), to the payment service provider's objectively justified reasons that gave rise to the suspicion of fraudulent behaviour on basis of that data, and to notifications made by the payment service provider to a provider of hosting services in accordance with Article 16 of Regulation EU/2022/2065. Information on the environmental and behavioural characteristics which are typical of the payer in the circumstances of a normal use of the personalised security credentials shall be excluded from information sharing under this Article.

2. Payment service providers shall implement appropriate technical and organisational measures, including measures to allow pseudonymisation, to ensure a level of security and confidentiality proportionate to the nature and extent of the information exchanged.

3. Payment service providers shall not keep data obtained following the information exchange referred to in paragraph 1 for longer than it is necessary for the purposes laid down in Article 83(1), point (c), and in any case no longer than 5 years after the suspected fraudulent transaction has taken place.

4. The information sharing arrangements shall specify the details of participation and the details of operational elements, including the use of dedicated IT platforms. Before concluding such arrangements, payment service providers shall jointly carry out a data protection impact assessment in accordance with Article 35 of Regulation (EU) 2016/679 and, where applicable, prior consultation of the supervisory authority in accordance with Article 36 of that Regulation.

5. Payment service providers shall not draw conclusions or take decisions that have an impact on a business relationship with the payment service user, such as terminating the contractual relationship with the user or affecting their future onboarding, solely on the basis of information received from other payment service providers who are subject to an information sharing arrangement without having assessed that information.

Article 83b

Platform on combatting fraud

1. The Commission shall establish a platform on combatting fraud in the area of payments services in the Union (the 'Platform'). Its composition shall be a broad and balanced mix of representatives and experts from both the public and private sectors, who have proven knowledge and experience in the field of payment services fraud.

2. The Platform shall:

(a) advise the Commission on developing and monitoring the implementation of legal acts aimed at combatting fraud in the area of payment services;

(b) issue recommendations to the Commission and the European Board of Digital Services for the purpose of the drawing up of the voluntary code of conduct referred to in Article 59a(2);

(c) share information on and analyse trends in fraud in the area of payment services;

(d) share information on measures to combat fraud in the area of payments services, including mitigation measures;

(e) share information on ways to improve cross-border and cross-sectoral cooperation on the means of combatting fraud in the area of payment services.

3. The Platform shall be chaired by the Commission and constituted in accordance with the horizontal rules on the creation and operation of Commission expert groups.

4. The Platform shall report annually on its activities to the European Parliament, the Council and the Commission.

Article 84

Payment fraud risks and trends

1. Payment service providers shall alert their customers via all appropriate means and media when new forms of payment fraud emerge, taking into account the needs of their most vulnerable groups of customers. Payment service providers shall give their customers clear indications on how to identify fraudulent attempts and warn them as to the necessary actions and precautions to be taken to avoid falling victim of fraudulent actions targeting them. Payment service providers shall inform their customers of where they can report fraudulent actions and rapidly obtain fraud-related information.

1a. Member States shall have in place adequate measures with appropriate funding to raise awareness among the public about the trends and new forms of payment fraud, the procedures to be followed in order to identify fraudulent attempts and the rights and obligations conferred by this Regulation relating to fraud. Member States shall ensure that communication measures are sufficient and well-targeted, in particular reaching out to the most vulnerable consumer groups, including younger and older persons and those with low digital skills. Member States shall inform the Commission about the measures taken.

Payment service providers, providers of very large online platforms or of very large online search engines and electronic communications service providers as defined in Article 2(4), point (b), of Directive (EU) 2018/1972 shall cooperate free of charge with the Member States in the measures referred to in subparagraph 1.

2. Payment service providers shall ***organise*** at least annually training programmes on payment fraud risks and trends for their employees ***that are active in designing, maintaining or offering payment services,*** and shall ensure that their employees are adequately trained to carry out their tasks and responsibilities in accordance with the relevant security policies and procedures to mitigate and manage payment fraud risks.

Article 85

Strong customer authentication

1. A payment service provider shall apply strong customer authentication where the payer:

   (a) accesses its payment account online;

   ▌

   (c) places a payment order for an electronic payment transaction;

   (d) carries out any ***other*** action through a remote channel which ***might*** imply a risk of payment fraud or other abuses***, including ordering the creation or replacement of a tokenised payment instrument via a remote channel, increasing its spending limits according to Article 51, changing its password online or changing its contact information online***.

2. Payment transactions that are ▌ initiated by the ▌ payee ▌ shall not be subject to strong customer authentication to the extent that those transactions are initiated without any interaction or involvement of the payer. ***Refunds that are initiated by the original payee in favour of the original payer against such transactions shall not be subject to strong customer authentication.***

▌

5. Where the mandate of the payer to the payee to place payment orders for ***merchant initiated*** transactions ▌ is provided through a remote channel with the involvement of the payment service provider, the setting up of such a mandate shall be subject to strong customer authentication.

6. For direct debits, where the mandate given by the payer to the payee to initiate one or several direct debit transactions is provided through a remote channel with the direct involvement of ***the payer's*** payment service provider in ▌ setting up of such a mandate ***shall be subject to*** strong customer authentication ▌ .

7. ***MOTO*** transactions ▌ shall not be subject to strong customer authentication ▌ , provided that security requirements and checks are carried out by the payment service provider of the payer allowing a form of authentication of the payment transaction.

8. For the remote placement of a payment order as referred to in paragraph 1, point (c), payment service providers shall apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

9. For the placement of a payment order as referred to in paragraph 1, point (c), through a payer's device using proximity technology for the exchange of information with the payee's infrastructure, the authentication of which requires the use of internet on the payer's device, payment service providers shall apply strong customer authentication that includes 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 the amount of the transaction and the payee throughout all of the phases of initiation.

10. For the purposes of paragraph 1, payment service providers shall have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

11. Any exemptions from the application of strong customer authentication to be designed by the EBA under Article 89 shall be based on one or more of the following criteria:

(a) the level of ***fraud*** risk involved in the service provided***, in particular based on the transaction monitoring mechanism as set out in Article 83***;

(b) the amount, the recurrence of the transaction, or both;

(c) the payment channel used for the execution of the transaction***,***

(ca) whether or not the payer is a consumer.

Exemptions from the application of strong customer authentication shall not be mandatory. A payment service provider implementing an exemption always retains the right to decide that under the circumstances and based on a risk assessment, strong customer authentication is necessary.

12. The two or more elements referred to in Article 3, point (35), on which strong customer authentication shall be based need to belong to different categories, ***except for the category inherence, where payment service provider can implement strong customer authentication using two elements only from this category, if it demonstrates to the national competent authority that the*** independence ***of the elements is at all times fully preserved and the authentication procedure ensures at all times a high level of security. The EBA shall develop guidelines by [18 months after entry into force of this Regulation] in accordance with Article 16 of the Regulation 1093/2010 on how to assess that the independence of the two inherence elements*** is fully preserved.

Article 85a

Strong customer authentication in respect of credit transfers

1. By derogation from Article 85(1), point (c), in the context of one or several recurring credit transfers initiated by the payer's payment service provider in accordance with this Article, the obligation to apply strong customer authentication shall not apply where the following cumulative conditions are met:

(a) the credit transfers are initiated by the payment service provider of the payer following a request from the payee;

(b) the payee's request is based on an agreement between the payer and the payee in which the payment conditions regarding frequency and amounts paid are set out, including where the amounts can vary, the circumstances in which the amounts can vary;

(c) the payer agrees that its payment service provider executes the respective credit transfers in line with the agreement mentioned in point (b) and the setting up of such agreement is subject to strong customer authentication;

(d) no additional action is required from the payer to initiate of the respective credit transfers.

2. In the case referred to in paragraph 1, the provisions referred to in Articles 61, 62 and 63 shall apply, with the exception of Article 62(1), fourth subparagraph.

Article 86

Strong customer authentication in respect of payment initiation and account information services

1. Article ***85(8), (9) and (12)*** shall also apply where payments are initiated through a payment initiation service provider. Article 85(10) shall also apply where payments are initiated through a payment initiation service provider and when the information is requested through an account information service provider.

2. Account servicing payment service providers shall allow payment initiation service providers and the account information service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with Article 85(1) and (10) and, where the payment initiation service provider is involved, in accordance with Article 85(1), (8), (9), (10) and (***12***).

3. Without prejudice to paragraph 2, where payment account information is accessed by an account information service provider, the account servicing payment service provider shall only apply strong customer authentication for the first access to payment account data by a given account information service provider, ▌ but not for the subsequent access to that payment account by that account information service provider ***unless the account servicing payment service provider has reasonable grounds to suspect fraud***.

4. ▌ Account information service providers shall apply ▌ strong customer authentication when the payment services user accesses the payment account information ***using*** that account information service provider at least 180 days after strong customer authentication was last applied. ***Account information service providers may apply their own or the account servicing payment service provider's strong customer authentication.***

Article 87

Outsourcing agreements for the application of strong customer authentication

1. ***The*** payment service provider ***of the payer*** shall enter into an outsourcing agreement with ***the*** technical service provider in case that technical service provider is providing and verifying the elements of strong customer authentication.

Article 88

Accessibility requirements regarding strong customer authentication

1. Without prejudice to the accessibility requirements under Directive (EU) 2019/882, payment service providers shall ensure that all their customers, including persons with disabilities, older persons, with low digital skills and those who do not have access to digital channels or payment instruments, have at their disposal at least a means, adapted to their specific situation, which enables them to perform strong customer authentication ***free of charge***. ***In case the payment service user requests help or is in need of assistance, the payment service provider shall ensure that support is provided. This requirement does not extend to providing devices to the payment service user. Payment service providers shall ensure that payment service users are adequately informed about the different means available to them to perform strong customer authentication.***

2. Payment services providers shall not make the performance of strong customer authentication dependant on the exclusive use of a single means of authentication and shall not make the performance of strong customer authentication depend, explicitly or implicitly, on the possession of a smartphone ***or other smart device, unless the payment service user has agreed to the provision of services exclusively through mobile applications on such device***. Payment services providers shall develop ***more than one*** means for ***the*** application of strong customer authentication to cater for the specific situation of all their customers ***including those referred to in paragraph 1***.

Article 88a

Fair, reasonable and non-discriminatory access to mobile devices

1. Without prejudice to Article 6(7) of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, original equipment manufacturers of mobile devices and electronic communications service providers within the meaning of Article 2(4) of Directive (EU) 2018/1972 shall allow payment service providers and technical services providers acting on their behalf effective interoperability with, and access for the purposes of interoperability to, the technical features, such as hardware features and software features, that are necessary to processing and executing securely payment transactions, on fair, reasonable and non-discriminatory terms.

2. Original equipment manufacturers of mobile devices and electronic communications service providers referred to in paragraph 1 shall not be prevented from taking strictly necessary and proportionate measures to ensure that interoperability does not compromise the integrity of the hardware and software features concerned by the interoperability obligation provided that such measures are duly justified.

3. For the purpose of applying fair, reasonable and non-discriminatory terms pursuant to paragraph 1, original equipment manufacturers of mobile devices and electronic communications service providers referred to in that paragraph shall publish general conditions of effective interoperability and access.

Article 89

Regulatory technical standards on authentication, communication and transaction monitoring mechanisms

1. The EBA shall develop draft regulatory technical standards which shall specify:

   (a) the requirements of strong customer authentication as referred to in Article 85;

   (b) the exemptions from the application of Article 85(1), (8) and (9), based on the criteria laid down in Article 85(11);

   (c) the requirements with which security measures have to comply, in accordance with Article 85(10) in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials;

(d) the requirements applicable, in accordance with Article 87, to the outsourcing agreements between the payers' payments service providers and technical service providers concerning the provision and verification of the elements of strong customer authentication by technical service providers;

(e) the requirements under Title III, Chapter 3 for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers;

(f) supplementary provisions on secure open standards of communication using dedicated interfaces;

(g) the technical requirements for transaction monitoring mechanisms referred to in Article 83.

For the purposes of point (b), as regards the exemption from the application of strong customer authentication for payment transactions, based on transaction risk analysis the draft regulatory technical standards shall specify, inter alia:

(i) the conditions that have to be met for a remote electronic payment transaction to be considered as posing a low level of risk;

(ii) the methodologies and models to implement transaction risk analysis;

(iii) the criteria for the calculation of fraud rates, including on the allocation of fraud rates between payment service providers providing issuing and acquiring services, or within payment service providers providing issuing and acquiring services through a single legal entity;

(iv) detailed and proportionate reporting and audit requirements.

▌

2. When developing the draft regulatory technical standards referred to in paragraph 1, the EBA shall take into account:

(a) the need to ensure an appropriate level of security for payment service users and payment service providers, through the adoption of effective and risk-based requirements;

(b) the need to ensure the safety of payment service users' funds and personal data;

(c) the need to secure and maintain fair competition among all payment service providers;

(d) the need to ensure technology and business-model neutrality;

(e) the need to allow for the development of user-friendly, accessible and innovative means of payment***;***

(ea) the need to balance fraud risk in a service or economic activity concerned with the consumer experience, in particular with regards to low value transactions;

(eb) whether or not the payers in the transactions are consumers.

The EBA shall submit the draft regulatory technical standards referred to in paragraph 1 to the Commission by [OP please insert the date= 1 year after the date of entry into force of this Regulation]. Power is delegated on 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.

3. In accordance with Article 10 of Regulation (EU) No 1093/2010, the EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments, and the provisions of Chapter II of Regulation (EU) 2022/2554, and the European Digital Identity Wallets implemented under Regulation (EU) No 910/2014.

CHAPTER 8

Enforcement procedures, competent authorities and penalties

Article 89a

Enforcement of provisions related to very large online platforms and very large online search engines

The Commission shall have exclusive powers to supervise and enforce Article 59a(3), third sub-paragraph, point (iii), and Article 59b of this Regulation, where the obligations in those provisions apply to providers of very large online platforms and very large online search engines within the meaning of Article 33 of Regulation (EU) 2022/2065. Chapter IV of Regulation (EU) 2022/2065 shall apply for the purposes of that supervision and enforcement and any references therein to compliance with the relevant provisions of Regulation (EU) 2022/2065 shall be deemed to include Article 59a(3), third sub-paragraph, point (iii), and Article 59b of this Regulation, where the obligations in those provisions apply to providers of very large online platforms and very large online search engines. To the extent that powers are conferred upon the Commission under Chapter IV of Regulation (EU) 2022/2065, those powers shall also cover the application of Article 59a (3), third sub-paragraph, point (iii), and Article 59b of this Regulation, where those obligations apply to providers of very large online platforms and very large online search engines.

SECTION -1

PROHIBITION OF PERSONS OTHER THAN PAYMENT SERVICE PROVIDERS FROM PROVIDING PAYMENT SERVICES

Article 89b

Prohibition of persons other than payment service providers from providing payment services

Natural or legal persons that are neither authorised payment service providers under [PSD3] nor exempted from such authorisation shall be prohibited from providing payment services.

SECTION 1

COMPLAINT PROCEDURES *AND INVESTIGATORY POWERS*

Article 90

Complaints

1. Member States shall set up procedures which allow payment service users and other interested parties including consumer associations, to submit complaints to the competent authorities designated to ensure enforcement of this Regulation, with regard to payment service providers' alleged infringements of the provisions of this Regulation.

2. Where appropriate and without prejudice to the right to bring proceedings before a court in accordance with national procedural law, the reply from the competent authorities to the complaints referred to in paragraph 1 shall inform the complainant of the existence of the alternative dispute resolution (ADR) procedures set up in accordance with Article 95.

Article 91

Competent authorities and *supervisory and* investigatory powers

-1. Member States shall designate the competent authorities responsible for carrying out the functions and duties provided for in this Regulation. Member States shall notify those competent authorities to the EBA and the Commission.

-1a. Where Member States designate more than one competent authority pursuant to paragraph -1, they shall determine their respective tasks and designate one competent authority as the single point of contact for cross-border administrative cooperation between competent authorities as well as with the EBA. Member States may designate a different single point of contact for each of those types of administrative cooperation.

1. Competent authorities shall exercise their powers to investigate potential infringements of this Regulation, and impose administrative ***penalties, periodic penalty payments and other*** administrative measures laid down in their national legal frameworks in accordance with this Regulation, in any of the following ways:

   (a) directly;

   (b) in collaboration with other authorities;

   (c) by delegating powers to other authorities or bodies, while retaining the responsibility for overseeing the delegated authority or body;

   (d) by applying to the competent judicial authorities.

Where competent authorities delegate the exercise of their powers to other authorities or bodies in accordance with point (c) the delegation of power shall specify the delegated tasks, the conditions under which they are to be carried out, and the conditions under which the delegation of power may be revoked. The authorities or bodies to which the powers are delegated shall be organised in such a manner as to ensure that conflicts of interest are avoided. Competent authorities shall oversee the activity of the authorities or bodies to which the powers are delegated.

2. ***The*** competent authorities ***designated under paragraph -1 of this Article shall take all appropriate measures*** to ensure and monitor effective compliance with this Regulation.

The competent authorities shall be either:

(a) public authorities;

(b) bodies recognised by national law or by public authorities expressly empowered for that purpose by national law, including national central banks.

The competent authorities shall be independent from economic bodies and avoid conflicts of interest. Without prejudice to paragraph 2, point (b), payment institutions, credit institutions, or post office giro institutions shall not be designated as competent authorities.

3. The competent authorities referred to in paragraph 1shall ***have all supervisory and*** investigatory powers and adequate resources necessary for the ***exercise*** of their ***functions***.

Those powers shall include ***at least***:

(a) in the course of procedures to investigate potential breaches of this Regulation, the power to require from, inter alia, the following natural or legal persons, all information necessary ***for the performance of the duties of the competent authorities***:

(i) payment services providers;

(ii) technical service providers***, payment scheme operators*** and payment system operators ***that are not covered by Regulation (EU) 2025/1355, without prejudice to the oversight of the operations of those payment systems by the Eurosystem or central banks of Member States whose currency is not the euro***;

(iii) ATM deployers which do not service payment accounts;

(iv) ***providers of*** electronic communications services ***as defined in Article 2(4), point (b), of Directive (EU) 2018/1972***;

(v) natural persons belonging to the entities referred to in points (i), (ii) and (iii);

(vi) third parties to whom the entities referred to in points (i), (ii) and (iii) have outsourced operational functions or activities;

(vii) agents and ***branches*** of the entities referred to in points (i), (ii) and (iii) ***that are*** established in the Member State concerned;

(viii) insofar as permitted by national law, any other person, in particular those involved in the initiation, processing or execution of payment services;

(b) the power to conduct all necessary investigations of any person referred to in points (a) (i) to (***viii***) established or located in the Member State of the competent authority or providing services therein, where necessary to carry out the tasks of the competent authorities, including the power to:

(i) require the submission of documents;

(ii) examine the books and records of the persons referred to in points (a) (i) to (vii) and take copies or extracts from such books and records;

(iii) obtain written or oral explanations from any person referred to in points (a) (i) to (vii) or their representatives or staff, where applicable;

(iv) interview any other natural person who consents to be interviewed for the purpose of collecting information relating to the subject matter of an investigation;

(c) the power to conduct all necessary inspections at the ▌ premises of the legal persons ***and at sites other than the private residence*** of the natural persons referred to in ***point (a)***, subject to the prior notification of the competent authorities concerned.

(d) to enter the premises of natural and legal persons, in accordance with national law, in order to seize items, documents and data in any form where a reasonable suspicion exists that items, documents or data relating to the subject matter of the inspection or investigation might be necessary and relevant to prove a case of breach of provisions of this Regulation;

(e) to require, insofar as permitted by national law, existing data traffic records held by a telecommunications operator, where there is a reasonable suspicion of a breach and where such records may be necessary for the investigation of a breach of this Regulation;

(f) to request the freezing or sequestration of assets, or both;

(g) to refer matters for criminal investigation;

(h) in the absence of other available means to bring about the cessation or the prevention of any breach of this Regulation and in order to avoid the risk of serious harm to the interests of consumers, insofar as permitted by national law and in accordance where applicable with Article 9 of Regulation (EU) 2022/2065, to take any of the following measures, including by requesting a third party or other public authority to implement them:

(i) to issue an order to remove content or to restrict access to an online interface or to display a warning that is explicitly displayed to customers when they access an online interface;

(ii) to order a hosting service provider to remove or disable access to an online interface;

(iii) to order domain registries or registrars to delete a fully qualified domain name and to allow the competent authority concerned to register it.

(i) to prohibit an offer of payment services where competent authorities find that this Regulation has been infringed or where there are reasonable grounds for suspecting that it will be infringed;

(j) to suspend or prohibit marketing communications where there are reasonable grounds for suspecting that this Regulation has been infringed;

(k) to prohibit the provision of payment services where they find that this Regulation has been infringed;

(l) where there is a reason to assume that a person is providing payment services without the required authorisation or the required registration, to order the immediate cessation of the activity without prior warning or imposition of a deadline;

(m) issue public notices;

For the purposes of point (m), if the information published by the competent authority proves to be false or the underlying circumstances incorrect, the competent authority shall inform the public of this in the same way as it previously published the information in question.

3a. The EBA shall publish on its website a list of the competent authorities designated in accordance with paragraphs 1 and 2.

4. Where the law of a Member State lays down criminal sanctions applicable to infringements of this Regulation in accordance with Article 96, ***paragraphs (1) and*** (2), that Member State shall have in place the necessary laws, regulations and administrative provisions to enable competent authorities:

(a) to liaise with competent judicial authorities in order to receive specific information regarding criminal investigations of alleged infringements of this Regulation, criminal proceedings commenced in respect of such alleged infringements, and the outcome of such proceedings including the final judgement;

(b) to provide such information to other competent authorities and the EBA to fulfil their obligation of cooperating with each other and with the EBA for the purposes of this Regulation.

5. The implementation and the exercise of powers set out in this Article shall be proportionate and shall comply with Union and national law, including with applicable procedural safeguards and with the principles of the Charter of Fundamental Rights of the European Union. The investigation and enforcement measures adopted in application of this Regulation shall be appropriate to the nature and the overall actual or potential harm of the infringement.

6. By [***21 months from*** 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, on complaints procedures, including the channels for submission of complaints, the information requested from complainants, and the disclosure of the aggregate analysis of complaints referred to in Article 90(1).

Article 92

Professional secrecy

1. Without prejudice to cases covered by national criminal law, all persons who work or who have worked for competent authorities, and any experts acting on behalf of the competent authorities, shall be bound by the obligation of professional secrecy regarding the information related to investigations conducted by the competent authorities.

2. The information exchanged in accordance with Article 93 shall be subject to the obligation of professional secrecy by both the sharing and recipient authority.

2a. Articles 53 to 61 of Directive 2013/36/EU shall apply mutatis mutandis.

2b. ***This Article shall not preclude the exchange of information between competent authorities and tax authorities in the same Member State, in accordance with national law. Where the information originates in another Member State, it shall only be exchanged as referred to in the first sentence of this paragraph with the express agreement of the competent authorities which have disclosed it.***

Article 93

Jurisdiction and cooperation of competent authorities

1. In the event of infringement or suspected infringement of Titles II and III, the competent authorities shall be those of the home Member State of the payment service provider, except for agents and branches conducting business under the right of establishment, where the competent authorities shall be those of the host Member State.

2. In the event of infringements or suspected infringements of Titles II and III by technical service providers, payment ***scheme operators, payment*** system operators***, processing entities,*** ATM deployers which do not service payment accounts, electronic communications services providers or by their agents or branches, the competent authorities shall be those of the Member State where the service concerned is provided.

3. In the exercise of their investigatory and sanctioning powers, including in cross border cases, competent authorities shall cooperate with each other [redacted] in accordance with Union and national law by exchanging information with each other and ensuring the mutual assistance to other competent authorities concerned as necessary for the effective enforcement of administrative sanctions and administrative measures.

4. The authorities from other sectors concerned, referred to in paragraph 3, shall cooperate with competent authorities for the effective enforcement of administrative sanctions and administrative measures.

[redacted]

SECTION 2

DISPUTE RESOLUTION PROCEDURES AND PENALTIES

Article 94

Dispute resolution

1. Payment service providers shall put in place and apply adequate and effective complaint resolution procedures for the settlement of complaints of payment service users concerning the rights and obligations under Titles II and III. The competent authorities shall monitor the performance of those procedures.

   Those procedures shall be applied in every Member State where the payment service provider offers the payment services and shall be available in an official language of the relevant Member State or in another language if agreed between the payment service provider and the payment service user.

2. Payment service providers shall ▌ reply, on paper or, if agreed between the payment service provider and the payment service user, on another durable medium, to the payment service users' complaints. Such a reply shall address all points raised, within an adequate timeframe and at the latest within 15 business days of receipt of the complaint. In exceptional situations, if the answer cannot be given within 15 business days for reasons beyond the control of the payment service provider, it shall send a holding reply, clearly indicating the reasons for a delay in answering to the complaint and specifying the deadline by which the payment service user will receive the final reply. In any event, the deadline for receiving the final reply shall not exceed 35 business days.

Member States may introduce or maintain rules on dispute resolution procedures that are more advantageous to the payment service user than that referred to in the first subparagraph. Where Member States do so, those rules shall apply.

3. The payment service provider shall inform the payment service user about at least one ADR entity which is competent to deal with disputes concerning the rights and obligations under Titles II and III.

4. The information referred to in paragraph 3 shall be mentioned in a clear, comprehensive and easily accessible way on the website of the payment service provider and on the respective mobile application, where they exist, at the branch, and in the general terms and conditions of the contract between the payment service provider and the payment service user. The payment service provider shall specify how further information on the ADR entity concerned and on the conditions for using it can be accessed.

Article 95

ADR procedures

1. Member States shall establish adequate, independent, impartial, transparent and effective ADR procedures for the settlement of disputes between payment service users and payment service providers concerning the rights and obligations under Titles II and III according to the relevant Union and national law in accordance with the quality requirements laid down in Directive 2013/11/EU of the European Parliament and the Council[29], using existing competent bodies where appropriate. ADR procedures shall be applicable to payment service providers.

The first subparagraph and paragraph 1a are without prejudice to the right of the payment service user concerned to initiate proceedings to contest the disputed payment transaction by the payment service providers before a court in accordance with the applicable law.

1a. The participation of payment service providers in ADR procedures for consumers shall be mandatory, unless the Member State demonstrates to the Commission that other mechanisms are equally effective.

2. The bodies referred to in paragraph 1 of this Article shall cooperate effectively for the resolution of cross-border disputes concerning the rights and obligations under Titles II and III.

---

[29] 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 (Directive on consumer ADR) (OJ L 165, 18.6.2013, p. 63).

3. Member States shall designate a competent authority ***in line with Article 18 of Directive 2013/11/EU which shall carry out the functions set out in Articles 19 and 20 of that Directive as regards*** ADR entity or entities on their territory to resolve disputes concerning rights and obligations under Titles II and III ***of this Regulation***.

4. Competent authorities, referred to in paragraph 3 shall notify ADR entity or entities in their territories to resolve disputes concerning rights and obligations under Titles II and III to the Commission, in line with Article 20 of Directive 2013/11/EU.

5. The Commission shall make publicly available a list of the ADR entities notified to it in accordance with paragraph 4 and update that list whenever changes are communicated. ***Member States shall make publicly available a hyperlink to the website of the Commission containing the information referred to in the first subparagraph.***

Article 96

Administrative sanctions and administrative measures

1. Without prejudice to the supervisory powers of competent authorities designated under Directive (EU) XXX (PSD3), in accordance with Title II, Chapter 1, section 3 of that Directive, and the right of Member States to lay down criminal sanctions, Member States shall lay down rules on administrative sanctions and administrative measures applicable to infringements of this Regulation and shall ensure that they are implemented. The administrative sanctions and administrative measures shall be effective, proportionate and dissuasive.

2. Member States may decide not to lay down rules on administrative sanctions and administrative measures applicable to breaches of this Regulation which are subject to sanctions under national criminal law. In such a case, Member States shall notify the Commission of the relevant criminal law provisions and any subsequent amendments thereto in accordance with Article 103.

3. Where the national rules referred to in paragraph 1 apply to payment service providers and other legal persons, in case of infringements and subject to the conditions laid down in national law, administrative sanctions and administrative measures shall be applicable to the members of the management body of such payment services providers and legal persons and to other natural persons found to be responsible for a breach of this Regulation.

4. Member States may lay down rules, in accordance with their national law, enabling their competent authorities to close an investigation concerning an alleged infringement of this Regulation, following a settlement agreement or an expedited enforcement procedure.

The empowerment of competent authorities to settle or open expedite enforcement procedures does not affect the obligations upon Member States under paragraph 1.

Paragraphs 1, 3 and 4 of this Article shall apply to the administrative sanctions and other administrative measures laid down in Article 97.

Article 97

Administrative sanctions and other administrative measures for specific infringements

1. Without prejudice to Article 96(2), national laws, regulations and administrative provisions shall lay down the administrative sanctions and other administrative measures referred to in paragraph 2 of this Article in respect of the breaching ▌ of the following provisions:

   (a) the rules on access to accounts maintained with a credit institution laid down in Article 32;

   (b) the ▌ rules ***on*** account information ***services*** and payment initiation ***services*** laid down in ▌ Title III, Chapter 3 ▌ ;

   (c) the obligation to organise or perform fraud prevention mechanisms**,** including strong customer authentication as set out in Articles 85, 86 and 87;

   (d) the duty to comply with the requirements for transparency on fees by ATM operators or other cash distributors, in accordance with Article 20(c) point (ii);

   (e) failure of payment service providers to respect the period for compensation of payment service users as set out in Article 56(2), Article 57(2)**,** Article 59(2) ***and Article 63(2)***.

2. In the cases referred to in paragraph 1, the applicable administrative sanctions and administrative measures shall include the following:

(a) administrative fines;

(i) in the case of a legal person, a maximum administrative fine of at least 10% of its total annual turnover as defined under paragraph 3;

(ii) in the case of a natural person, a maximum administrative fine of at least EUR ***3 000 000***, or in the Member States whose currency is not the euro, the corresponding value in the national currency on the date of entry into force of this Regulation;

(iii) a maximum administrative fine of at least twice the amount of the profits gained from ***or losses avoided because of*** the breach, where ***those profits or losses*** can be determined***, even if such fine exceeds the maximum amounts set out in this paragraph, point (i), as regards legal persons, or in point (ii) as regards natural persons***.

(b) a public statement indicating the legal or natural person responsible for the breach and the nature of the breach;

(c) an order requiring the legal or natural person responsible for the breach to cease the unlawful conduct and to desist from repeating it;

(d) a temporary ban preventing a member of the management body of the legal person, or any other natural person who is held responsible for the breach, from exercising managing functions.

3. The total annual turnover referred to in paragraph 2, point (a)(i) of this Article and in Article 98(1) of this Regulation shall be equal to the net turnover as defined in Article 2, point (5), of Directive 2013/34/EU according to the annual financial statements available for the latest balance sheet date, for which the members of the administrative, management and supervisory bodies of the legal person have responsibility.

Where the legal person is a parent undertaking or a subsidiary of a parent undertaking which is required to prepare consolidated financial statements in accordance with Article 22 of Directive 2013/34/EU, the relevant total annual turnover shall be the net turnover or the revenue to be determined in accordance with the relevant accounting standards, according to the consolidated financial statements of the ultimate parent undertaking available for the latest balance sheet date, for which the members of the administrative, management and supervisory body of the ultimate undertaking have responsibility.

4. Member States may empower competent authorities, in accordance with national law, to impose other types of ***administrative measures and*** sanctions and other type of sanctioning powers in addition to those referred to in paragraph 2 of this Article ▌ .

Article 98

Periodic penalty payments

1. Competent authorities shall be entitled to impose periodic penalty payments on legal or natural persons for ***ongoing breaches of this Regulation or breaches of any decisions issued by a competent authority*** in accordance with this Regulation.

   Periodic penalty payment referred to in the first subparagraph shall be effective and proportionate and shall consist of a daily amount to be paid until compliance is restored. They shall be imposed for a period not exceeding 6 months from the date indicated in the decision imposing the periodic penalty payments.

   Competent authorities shall be entitled to impose maximum periodic penalty payments of at least:

   (a) 3% of the average daily turnover in the case of a legal person;

   (b) EUR 30.000 in the case of a natural person.

   The average daily turnover shall be the total annual turnover referred to in Article 97(3), divided by 365. ***Where a periodic penalty payment is imposed on a credit institution, the average daily turnover shall be the total annual turnover referred to in Articles 66(3) and 67(3) of Directive 2013/36/EU, divided by 365.***

2. Member States may provide for higher amounts of pecuniary penalty payments than those laid down in paragraph 1.

Article 99

Elements to be considered when determining administrative sanctions and other administrative measures

1. Competent authorities, when determining the type and level of administrative sanctions or other administrative measures, shall take into account all relevant elements and circumstances to apply proportionate sanctions, including:

   (a) the seriousness and the duration of the infringement;

   (b) the degree of responsibility of the natural or legal person responsible for the infringement;

   (c) the financial strength of the natural or legal person responsible for the breach, as indicated, among others, by the total annual turnover of the legal person, or the annual income of the natural person responsible for the infringement;

(d) the magnitude of profits gained or losses avoided by the natural or legal person responsible for the infringement, insofar as they can be determined;

(e) the losses for third parties resulted from the infringement, insofar as they can be determined;

(f) ***criminal penalties previously imposed for the same breach on the*** natural ***or legal*** person responsible for ***that*** breach ▌ ;

(g) the impact of the infringement in the interests of consumers and other payment services users;

(h) any actual or potential systemic negative consequences of the infringement;

(i) the complicity or participation of more than one natural or legal person in the infringement;

(j) previous ***breaches*** by the natural or legal person responsible for the breach;

(k) the level of cooperation of the natural or legal person responsible for the infringement with the competent authority;

(l) any remedial action or measure undertaken by the legal or natural person responsible for the infringement to prevent its repetition.

2. Competent authorities that use settlement agreements or expedited enforcement procedures in accordance with Article 96(4) shall adapt the relevant administrative sanctions and administrative measures laid down in Articles 96 ***and 97*** and ***periodic penalty payments laid down in Article*** 98 to the case concerned to ensure the proportionality thereof.

Article 100

Right of appeal

1. The decisions ***to impose administrative measure or administrative sanction*** taken by the competent authorities pursuant to this Regulation shall be ***subject to appeal***.

2. Paragraph 1 shall apply also in respect of failure to act ***where this Regulation sets a fixed period for the competent authority to act***.

Article 101

Publication of administrative sanctions and administrative measures

1. Competent authorities shall publish on their website all decisions imposing an administrative sanction or administrative measure on legal and natural persons, for breaches of this Regulation, and where applicable, all settlement agreements. The publication shall include a short description of the breach, the administrative sanction or other administrative measure imposed, or, where applicable, a statement about the settlement agreement. The identity of the natural person subject to the decision imposing an administrative sanction or administrative measure ***or to the settlement agreement to which that natural person is a party,*** shall not be published.

   Competent authorities shall publish the decision and the statement referred to in the first subparagraph ***without undue delay*** after the legal or natural person subject to the decision has been notified of that decision or the settlement agreement has been signed.

2. By derogation from paragraph 1, where the publication of the identity or other personal data of natural persons is deemed necessary by the national competent authority to protect the stability of the financial markets or to ensure the effective enforcement of this Regulation, including in the case of public statements referred to in Article 97(2)(b) or temporary bans referred to in Article 97(2)(d), the national competent authority may publish also the identity of the persons or personal data provided that it justifies such a decision and that the publication is limited to the personal data that is strictly necessary to protect the stability of the financial markets or to ensure the effective enforcement of this Regulation.

3. Where the decision imposing an administrative sanction or other administrative measure is subject to appeal before the relevant judicial or other authority, competent authorities shall also publish on their official website without delay, information on the appeal and any subsequent information on the outcome of such an appeal, insofar as it concerns legal persons. Where the appealed decision concerns a natural person and the derogation under paragraph 2 is not applied, competent authorities shall publish information on the appeal only in an anonymised version.

4. Competent authorities shall ensure that any publication made in accordance with this Article remains on their official website for a period of ***at least*** 5 years. Personal data contained in the publication shall be kept on the official website of the competent authority only ***for the period which is necessary in accordance with the applicable data protection rules***.

Article 102

Monitoring of proceedings, sanctions and measures

1. Competent authorities shall report to the EBA, in an anonymised way and aggregated format on a regular basis:

   (a) initiated, suspended or closed formal administrative proceedings leading to imposing administrative sanctions or administrative measures ***for breaches of this Regulation***;

   (b) periodic penalty payments imposed in accordance with Article 98 for ongoing breaches of this Regulation;

   (c) where applicable, settlement agreements and expedited enforcement procedures, and the outcome thereof, regardless of their publication; in accordance with Article 96(4);

   (d) criminal proceedings resulting in a conviction and related sanctions reported by judicial authorities in accordance with Article 91(4), point (a);

   (e) any appeal against decisions to impose criminal or administrative sanctions or administrative measures ***for breaches of this Regulation*** and the outcome of such an appeal.

2. When the competent authority discloses an administrative sanction or an administrative measure to the public, it shall simultaneously report them to the EBA.

3. Within 2 years after the date of application of this Regulation, and subsequently every 2 years, the EBA shall submit a report to the Commission on the application of sanctions by competent authorities to ensure compliance with this Regulation.

Article 103

Notification of implementing measures

Member States shall notify the laws, regulations and administrative provisions adopted in accordance with this Chapter, including any relevant criminal law provisions, to the Commission by [***21 months from*** the date of entry into force of this Regulation]. Member States shall notify the Commission without undue delay of any subsequent amendments thereto.

CHAPTER 9

Product intervention powers by the EBA

Article 104

EBA temporary intervention powers

1. In accordance with Article 9(5) of Regulation (EU) No 1093/2010, the EBA may, where the conditions in paragraphs 2 and 3 of this Article are fulfilled, temporarily prohibit or restrict in the Union, a certain type or a specific feature of a payment service or instrument ▌. A prohibition or restriction may apply in circumstances, or be subject to exceptions, specified by the EBA.

2. The EBA shall take a decision under paragraph 1 only if all of the following conditions are fulfilled:

   (a) the proposed action addresses a significant number of payment ▌ services users or a threat to the orderly functioning of the payment or electronic money markets, and the integrity of those markets or to the stability of the whole or part of these markets in the Union;

(b) regulatory requirements under Union law that are applicable to the relevant payments service or electronic money service do not address the threat;

(c) a competent authority or competent authorities have not taken action to address the threat or the actions that have been taken do not adequately address the threat.

Where the conditions set out in the first subparagraph are fulfilled, the EBA may impose the prohibition or restriction referred to in paragraph 1 on a precautionary basis before a payment service or electronic money service has been offered or distributed to payment services users.

3. When taking action under this Article, the EBA shall ensure all of the following:

(a) the action does not have a detrimental effect on the efficiency of the payments market or electronic money ▌ market or on payment ▌ service providers that is disproportionate to the benefits of the action;

(b) the action does not create a risk of regulatory arbitrage, and

(c) the action has been taken after consulting the relevant national competent authority.

4. Before deciding to take any action under this Article, the EBA shall notify competent authorities of the action it proposes.

5. The EBA shall publish on its website notice of any decision to take any action under this Article. The notice shall specify details of the prohibition or restriction and specify a time after the publication of the notice from which the measures will take effect, while also ensuring that notices on such decisions on natural persons are published only in anonymised version. A prohibition or restriction shall only apply to action taken after the measures take effect.

6. The EBA shall review a prohibition or restriction imposed under paragraph 1 at appropriate intervals and at least every 3 months. If the prohibition or restriction is not renewed after that 3 month period it shall expire.

7. Action adopted by the EBA under this Article shall prevail over any previous action taken by a competent authority.

8. The Commission shall adopt delegated acts in accordance with Article 106 to specify criteria and factors to be taken into account by the EBA in determining when there is a significant number of payment services users or ▌ a threat to the orderly functioning of the payment or electronic money ▌ markets, and the integrity of these markets or to the stability of the whole or part of these markets in the Union referred to in paragraph 2, point (a).

Those criteria and factors shall include:

(a) the degree of complexity of a payment service or instrument or electronic money service or instrument and the relation to the type of users, including consumers, to whom they are offered;

(b) the degree of riskiness, for consumers, of a payment service or instrument or electronic money service or instrument;

(c) the possible use by fraudsters of the payment service or instrument or electronic money service or instrument;

(d) the size or the level of uptake of the payment service or instrument or electronic money service or instrument;

(e) the degree of innovation of a payment service or instrument or electronic money service or instrument.

TITLE IV
DELEGATED ACTS

I

Article 106

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in ***Articles 31a, 60, 67a and 104(8)*** shall be conferred on the Commission for an undetermined period of time from the date of entry into force of this Regulation.

3. The delegation of power referred to in ***Articles 31a, 60, 67a and 104(8)*** may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or on a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by Member States in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to ***Articles 31a, 60, 67a and 104(8)*** shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of 3 months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by 3 months at the initiative of the European Parliament or of the Council.

TITLE V
FINAL PROVISIONS

Article 107

More favourable refund rights and stricter fraud prevention measures

1. Member States or payment service providers may grant payment service users more favourable refund rights in relation to authorised credit transfers as referred to in Articles 57 and 59 and provide for stricter fraud prevention measures that go beyond those set out in Article 83(1) and Article 84.

2. Member States shall, by [OP please insert the date= the date of entry into force of this Regulation], notify to the Commission the provisions adopted pursuant to paragraph 1. They shall, without delay, notify any subsequent amendment to the Commission.

Article 108

Review clause

1. The Commission shall, by ***[OP please insert the date =*** *7* years after ***entry into force*** of this Regulation***]***, submit to the European Parliament, the Council, the ECB and the European Economic and Social Committee, a report on the application and impact of this Regulation, and in particular on:

   (a) the appropriateness and the impact on competition and the uptake of open banking of the rules on access to payment accounts data on the business of account information services and payment initiation services, and in particular of the rules on dedicated interfaces and their respective derogations as per Articles 38 and 39;

   (b) the impact of the rules on the absence of obligatory contractual arrangements and compensation for access by account information service and payment initiation service providers to interfaces referred to in Article 34;

(d) the appropriateness and impact of the rules on prevention and redress of fraud on both unauthorised and authorised transactions***, taking into account types and trends of fraudulent behaviours***.

(da) the appropriateness and impact of the rules on the extent of situations where a consumer has a refund right for authorised transactions in accordance with Article 59.

▌

Where appropriate, the Commission shall submit a legislative proposal together with its report.

1a. The Commission shall, by ... [5 years after entry into force of this Regulation], submit to the European Parliament, the Council, the ECB and the European Economic and Social Committee, a report reviewing:

- the impact of the surcharging provisions, including the effects on consumers, merchants, and competition, and shall assess the need for further harmonisation; and

- the impact of refund mechanisms managed by operators of payment schemes or payment service providers that are applicable to payee initiated transactions, with the exclusion of direct debits, as well as the effects of those refund mechanisms on consumers, merchants and competition;

- the impact of the provisions contained in Article 59a in relation to obligations imposed on electronic communications services providers in particular, whether those obligations improve the effectiveness of the cooperation between electronic communications services providers and payment service providers under Article 59a. On the basis of that assessment, the Commission shall determine whether it is necessary to introduce any further measures regulating the involvement of electronic communications services providers and payment service providers in the security of payment transactions at EU level;

- the impact of the provisions contained in Article 59a in relation to obligations imposed on providers of hosting services, very large online platforms and very large online search engines, in particular whether those obligations improve the effectiveness of the cooperation between providers of hosting services and payment service providers under Article 59a, 59b and the right of redress for PSPs under Article 78. On the basis of that assessment, the Commission shall determine whether it is necessary to introduce any further measures regulating the involvement of providers of hosting services, very large online platforms and very large online search engines, and payment service providers in the security of payment transactions at EU level.

Where appropriate, the Commission shall submit a legislative proposal together with its report.

1b. The Commission shall, by ... [3 years after entry into force of this Regulation], submit to the European Parliament, the Council, the ECB and the European Economic and Social Committee, a report assessing:

- the scope of this Regulation, with regard in particular to payment systems, payment schemes and technical service providers;

- whether, in light of the risks and challenges, including anti money laundering law enforcement perspectives, posed by virtual IBANs, including from an anti-money laundering law enforcement perspective, and of their benefits, it would be necessary to introduce further measures regulating virtual IBANs at EU level;

- the appropriateness and the impact of the rules set out in Titles II and III of this Regulation with regard to payment transactions with electronic money tokens;

- whether, given developments, it would be desirable, to extend the requirements in this Regulation on the verification of the payee and open banking to payment transactions with electronic money tokens.

Where appropriate, the Commission shall submit a legislative proposal together with its report.

2. The Commission shall, by [OP please insert the date= ***18 months*** after the date of entry into force of this Regulation] submit to the European Parliament, the Council, the ECB and the European Economic and Social Committee, a report on the ***practices of*** payment ***card schemes, processing entities***, payment ▌ service providers ***providing acquiring services and in particular on:***

(a) the evolution of their fees in the EEA; including: i. fees charged by payment card schemes and processing entities to payment service providers providing acquiring by key transaction category, per Member State, ii. fees charged by payment service providers providing acquiring services to business payment service users;

(b) the conditions related to the application of new rules and associated fees, such as notification period of these rules and fees by payment card schemes and processing entities;

(c) the communication by payment card schemes to payment service providers providing acquiring services and processing entities related to rules and fees and their implementation timeline;

(d) the capacity of issuers and acquirers to negotiate rules and fees proposed by payment card schemes;

(e) the competitive behaviour of the payment card schemes in the acquiring and issuing markets.

Where appropriate, the Commission shall submit a legislative proposal together with that report.

A non confidential version of the report shall be made available to the public, including but not limited to aggregate information on the evolution of fees.

▌

Article 108a

Transitional provisions

By way of derogation from Directive (EU) 2015/2366, until [21 months after the entry into force of this Regulation]:

(a) the following payment transactions shall be excluded from the application of Directive (EU) 2015/2366:

- payment transactions made exclusively in electronic money tokens directly from the payer to the payee, without any intermediary intervention;

- payments transactions carried out by a crypto-asset service provider intermediating between a buyer and a seller where electronic money tokens are exchanged for other electronic money tokens or for crypto-assets, as well as the exchange of electronic money tokens for funds, including electronic money tokens, or crypto-assets carried out by a crypto-asset service provider acting in its own name as buyer or seller of those electronic money tokens;

- payment transactions carried out between crypto-asset service providers or their branches for their own account.

(b) ***as regards payment transactions with electronic money tokens settled on the distributed ledger, where payment service providers are not able, due to circumstances that are not attributable to them, to comply with the obligations set out by Article 45(1), points (b) and (c), Article 52(2), point (e) and (3), point (a) and Article 56 of Directive (EU) 2015/2366, the payment service providers shall provide the information required therein by way of a reasoned estimation as soon as possible, and in any case prior to the payer authorising the transaction;***

(c) ***payment service providers shall not be required to apply Article 66(4) and Article 67(3) of Directive (EU) 2015/2366 as regards payment transactions with electronic money tokens.***

Article 109

Amendments to Regulation (EU) No 1093/2010

Regulation (EU) No 1093/2010 is amended as follows:

1. In Article 1(2), the first sentence is replaced by the following:

"The Authority shall act within the powers conferred by this Regulation and within the scope of Directive 2002/87/EC, Directive 2008/48/EC ([1]), Directive 2009/110/EC, Regulation (EU) No 575/2013 ([2]), Directive 2013/36/EU ([3]), Directive 2014/49/EU ([4]), Directive 2014/92/EU ([5]), Directive (EU) […] (PSD3), Regulation (EU) […] (PSR) of the European Parliament and of the Council and, to the extent that those acts apply to credit and financial institutions and the competent authorities that supervise them, within the relevant parts of Directive 2002/65/EC, including all directives, regulations, and decisions based on those acts, and of any further legally binding Union act which confers tasks on the Authority.;"

2. Article 4(2) is amended as follows:

(a) point (i) is replaced by the following:

'competent authorities or supervisory authorities within the scope of the sectoral acts referred to in Article 1(2), including the European Central Bank with regard to matters relating to the tasks conferred on it by Regulation (EU) No 1024/2013;'

(b) points (iii), (vi), (vii) and (viii) are deleted.

Article 110

Amendment to Regulation (EU) No 2017/2394

In the Annex to Regulation (EU) 2017/2394, the following point is added:

‘29. Regulation (EU) xxxx of the European Parliament and of the Council of xxxx on payment services in the internal market and amending Regulation (EU) No 1093/2010.’

Article 110a

Amendment to Regulation (EU) No 2021/1230

Regulation (EU) No 2021/1230 is amended as follows:

1. In Article 4, the first paragraph is replaced by the following:

‘1. With regard to the information requirements on currency conversion charges and the applicable exchange rate, as set out in Articles 13(1), 20(c), and 5(2) of Regulation (EU) [PSR] of the European Parliament and of the Council[30], payment service providers and parties providing currency conversion services at an automated teller machine (ATM) or at the point of sale, as referred to in Article 5(2) of that Regulation, shall express the total currency conversion charges as a monetary amount in the currency of the payer’s account and as a percentage mark-up over an aggregated mid-market exchange rate as referred to in Article 5(4) of that Regulation. That mark-up and any other applicable charges shall be disclosed to the payer prior to the initiation of the payment transaction.’;

---

30 OP: Please insert in the text the number of the Regulation contained in document 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 and Regulation (EU) No 2021/1230 - COM/2023/367 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.

2. In Article 5, the first paragraph is replaced by the following:

'1. When a currency conversion service is offered by the payer's payment service provider in relation to a credit transfer, as defined in point 28 of Article 3 of Regulation (EU) [PSR] of the European Parliament and of the Council[31], that is initiated online directly, using the website or the mobile banking application of the payment service provider, the payment service provider, with regard to Articles 13(1) and 20(c) of that Regulation, shall inform the payer prior to the initiation of the payment transaction, in a clear, neutral and comprehensible manner, of the estimated charges for currency conversion services and any other charges applicable to the credit transfer. The estimated charges for currency conversion in relation to credit transfers shall be expressed as a monetary amount in the currency of the payer's account and as a percentage mark-up over an aggregated mid-market exchange rate as referred to in Article 5(4) of that Regulation.'

[31] *OP: Please insert in the text the number of the Regulation contained in document 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 and Regulation (EU) No 2021/1230 - COM/2023/367 final) and insert the number, date, title and OJ reference of that Regulation in the footnote.*

Article 110b

Amendment to Regulation (EU) No 2023/1114

Article 60 is amended as follows:

The following paragraph 4a is inserted:

'4a. A payment institution may provide crypto-asset services in relation to e-money tokens for the purposes of providing payment services, where such crypto-asset services are deemed equivalent to those payment services for which the payment institution has been authorised under [PSD3] if it notifies the competent authority of the home Member State of the information referred to in paragraph 7 of this Article at least 40 working days before providing those crypto-asset services for the first time.

For the purpose of this paragraph:

providing custody and administration of crypto-assets on behalf of clients is deemed equivalent to the payment service of enabling cash to be placed on or withdrawn from a payment account referred to in point (1), of Annex I to [PSD3];

the exchange of crypto-assets for funds and other crypto-assets is deemed equivalent to the payment service of execution of payment transactions referred to in point (2), of Annex I of [PSD3];

providing transfer services for crypto-assets on behalf of clients is deemed equivalent to the payment service of execution of payment transactions referred to in point (2), of Annex I of [PSD3];

the execution of orders for crypto-assets on behalf of clients is deemed equivalent to the payment service of execution of payment transactions referred to in point (2), of Annex I of [PSD3];

the reception and transmission of orders for crypto-assets on behalf of clients is deemed equivalent to the payment initiation services referred to in point (6), of Annex I of [PSD3].'

Article 110c

Amendment to Regulation (EU) No 260/2012

1. In Article 2, the following point is added:

'(15a) 'virtual IBAN' means an identifier containing the elements specified by the ISO as referred to in point (15) and causing payments to be redirected to a payment account identified by an IBAN different from that identifier.' .

2. The following article is inserted:

'Article 2a

Payment account identifier

For the purposes of this Regulation a virtual IBAN shall be considered to be a valid payment account identifier where the use of an IBAN is required.'

3. Article 5c is amended as follows:

(a) paragraph 5 is replaced by the following:

'PSPs shall ensure that the performance of the service ensuring verification and of the service described in paragraph 2 does not prevent payers from authorising the credit transfer concerned, without prejudice to the third subparagraph of paragraph 6.'

(b) paragraph 6 is replaced by the following:

'PSPs shall provide PSUs that are not consumers with the means to opt out from receiving the service ensuring verification when submitting payment orders via payment initiation channels that are based on automated dedicated processes or protocols and that are only made available to PSUs that are not consumers.

PSPs shall ensure that PSUs that are not consumers that opted out from receiving the service ensuring verification have the right to opt in at any time to receive that service. In the case of payment orders submitted via payment initiation channels referred to in the first subparagraph, including multiple payment orders that are submitted as a package, PSPs shall offer PSUs that are not consumers the possibility of agreeing in the framework contract that:

(a) the service ensuring verification is provided after authorisation of those payment orders; and

(b) the payer's PSP executes those payment orders without any further input from the PSU only in one or more of the following cases:

> ***(i) the information received by the payer's PSP from the payee's PSP shows that that the name of the payee as provided by the payer matches the payment account identifier specified in point (1)(a) of the Annex;***
>
> ***(ii) the information received by the payer's PSP from the payee's PSP shows that that the name of the payee as provided by the payer almost matches the payment account identifier specified in point (1)(a) of the Annex;***
>
> ***(iii) the service ensuring verification cannot be provided because of technical reasons.***

The possibility for the PSU that is not a consumer to contractually agree that the payer's PSP executes payment orders as set out in the third subparagraph shall be without prejudice to the requirement in paragraph 1, point (a), for the payer's PSP to indicate to the payer, in cases where the name of the payee as provided by the payer almost matches the payment account identifier specified in point (1)(a) of the Annex provided by the payer, the name of the payee associated with that payment account identifier.

For the purposes of paragraph 8, where the payer's PSP proceeds to execute the payment orders in accordance with the framework contract as referred to in the third subparagraph, the payer's PSP shall not be deemed liable for not having complied with the requirement to offer the service ensuring payee verification. '

Article 111

Correlation table

Any reference to Directive (EU) 2015/2366 and to Directive 2009/110/EC shall be construed as a reference to Directive (EU) (PSD3) or to this Regulation and shall be read in accordance with the correlation table in ***the*** Annex ▌ to this Regulation.

Article 112

Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from [OP please insert the date= ***21*** months after the date of entry into force of this Regulation].

However, Articles 50 and 57 shall apply from [OP please insert the date= ***27*** months after the date of entry into force of this Regulation].

Articles 85a and 108a shall apply from the date of entry into force of this Regulation.

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at **.....**,

For the European Parliament
The President

For the Council
The President

L

L

Annex *I*

CORRELATION TABLE