Council of the
European Union

Brussels, 5 July 2023
(OR. en)

11222/23

Interinstitutional File:
2023/0210 (COD)

EF 200
ECOFIN 694
CODEC 1237

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	29 June 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2023) 367 final
Subject:	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

Delegations will find attached document COM(2023) 367 final.

Encl.: COM(2023) 367 final

EUROPEAN
COMMISSION

Brussels, 28.6.2023
COM(2023) 367 final

2023/0210 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on payment services in the internal market and amending Regulation (EU) No 1093/2010

(Text with EEA relevance)

{SEC(2023) 256 final} - {SWD(2023) 231 final} - {SWD(2023) 232 final}

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE PROPOSAL

• Reasons for and objectives of the proposal

The second Payment Services Directive (PSD2[1]) provides a legal framework for all retail payments in the EU, both Euro and other currencies, domestic and cross-border. The first Payment Services Directive (PSD1[2]), adopted in 2007, established a harmonised legal framework for the creation of an integrated EU payments market. Building on PSD1, PSD2 addressed barriers to new types of payment services and improved the level of consumer protection and security. Most of the rules in PSD2 have been applicable since January 2018, but some rules such as those on Strong Customer Authentication, (SCA) have only applied since September 2019.

PSD2 contains rules on the provision of payment services and rules on licensing and supervision of one category of payment service provider, namely Payment Institutions (PIs). Other categories of PSP include credit institutions, which are regulated under EU banking legislation[3], and electronic money institutions (EMIs), which are regulated under the Electronic Money Directive[4].

The Commission's 2020 Communication on a retail payments strategy (RPS) for the EU[5] laid down the Commission's priorities for the retail payments area for the term of office of the current College of Commissioners (2019-2024). It was accompanied by a Digital Finance Strategy, which sets out priorities for the digital agenda in the finance sector other than payments. The RPS announced that "*at the end of 2021, the Commission will launch a comprehensive review of the application and impact of PSD2*". This review was duly undertaken, essentially in 2022, and led to a decision by the Commission to propose legislative amendments to PSD2, to improve its functioning. These amendments are set out in two proposals, the present proposal for a Regulation on payment services in the EU and a proposal for a Directive on payment services and e-money services, focussing on licensing and supervision of payment institutions (and amending certain other Directives).

The proposed revision of PSD2 features in the Commission Work Programme for 2023, along with a planned legislative initiative on a framework for financial data access, extending financial data access and use beyond payment accounts to more financial services.

• Consistency with existing policy provisions in the policy area

Existing policy provisions of relevance to this initiative include other legislation in the area of payments, other financial services legislation covering also payment services providers and EU legislation of horizontal application which impacts the payments area. Care has been taken in the preparation of this proposal to ensuring coherence with those provisions.

Other legislation in the field of retail payments, apart from those mentioned above, includes the Single Euro Payments Area (SEPA) Regulation of 2012, which harmonises the technical

---

1 Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market.

2 Directive 2007/64/EC of 13 November 2007 on payment services in the internal market.

3 Regulation (EU) No 575/2013 on prudential requirements for credit institutions, Directive 2013/36/EU on access to the activity of credit institutions and the prudential supervision of credit institutions.

4 Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

5 COM (2020) 592 final, of 24 September 2020.

requirements for credit transfers and direct debits in euro[6]. On 26 October 2022, the Commission proposed an amendment to the SEPA Regulation, to accelerate and facilitate the use of instant payments in euro in the EU[7]; that proposal contains a requirement for payment services providers offering euro instant payments to offer to users an "IBAN/name verification service", and the present proposal extends that requirement to payment services providers offering any credit transfer in any EU currency. The Regulation on cross-border payments equalises pricing of domestic and cross-border transfers in euro[8]. The Regulation on Interchange Fees lays down maximum levels for such fees[9]. The present proposal is consistent with the objective of improving access to cash, by allowing merchants to offer, in physical shops, cash provision services even in the absence of a purchase by a customer. The work on access to cash is also to be seen in the context of the Commission's RPS, which stated as a policy objective that cash should remain widely accessible.

Other relevant financial services legislation includes the Settlement Finality Directive (SFD),[10] to which a targeted change is made in the proposal for a Directive accompanying this proposal. Other relevant legislation includes the Markets in Crypto-Assets Regulation (MiCA)[11], the Digital Operational Resilience Act concerning cyber-security (DORA)[12] and the Anti-Money Laundering (AML) Directive, of which a package of proposed amendments is currently under discussion by the co-legislators.[13]

The initiative is fully consistent with other Commission initiatives laid out in the Commission's digital finance strategy for the EU[14], which was adopted together with the RPS, and aims to promote digital transformation of finance and the EU economy and to remove fragmentation in the digital internal market.

- **Consistency with other EU policies**

The initiative is consistent with the Commission's 2021 Communication on 'The European economic and financial system: fostering openness, strength and resilience'[15] which reiterated the importance of the Commission's RPS and of digital innovation in finance for strengthening the internal market for financial services. The same Communication confirmed that the Commission and European Central Bank services would jointly review at technical level a broad range of policy, legal and technical questions arising from a possible introduction of a digital euro, taking into account their respective mandates under the EU Treaties.

The Commission is submitting a proposal for an EU legal framework on financial information data access (FIDA) is presented in conjunction with the proposals to amend PSD2; that proposal covers access to financial data other than payment account data, which remains covered by payments legislation.

---

6 Regulation (EU) No 260/2012 of 14 March 2012.
7 COM(2022) 546 final.
8 Regulation (EU) 2021/1230 of 14 July 2021 on cross-border payments in the Union.
9 Regulation (EU) 2015/751 of 29 April 2015 on interchange fees for card-based payment transactions.
10 Directive 98/26/EC of 19 May 1998 on settlement finality in payment and securities settlement systems.
11 Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets.
12 Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector.
13 Payment services providers are obliged entities in the meaning of EU AML legislation.
14 COM (2020) 591 final of 24 September 2020.
15 COM (2021) 32 final of 19 January 2021.

More general EU legislation of relevance includes GDPR[16], EU Accessibility Act[17], and the proposal for a Data Act, which is relevant for open banking[18]. In particular, Chapter III and IV of the proposed Data Act establish a horizontal framework for the rights and obligations with regard to the terms and conditions for making data available in business-to-business relations.

2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY

• Legal basis

The legal basis of PSD2 is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which tasks the EU institutions with laying down provisions to establish the internal market and ensure its proper functioning in line with Article 26 TFEU.

• Subsidiarity (for non-exclusive competence)

Payment services may also be provided cross-border by payment service providers within the internal market for payment services. The freedom to provide services and freedom of establishment are widely used by payment service providers. To ensure harmonious conditions and a level playing field within the internal market for retail payment services, EU-level legislation is required. This logic underlied the first and second Payment Services Directives and continues to apply to this proposal.

• Proportionality

The proposal contains targeted proportionality measures, such as the possibility, in the area of open banking, for an account servicing payment services provider (ASPSP) to obtain from its national competent authority a derogation from the requirement to have in place a dedicated interface for data access.

• Choice of the instrument

PSD2 is currently a directive which is applied by transposing legislation in the Member States. However, in various areas of EU financial services legislation[19], it has been found appropriate to enact rules applicable to financial undertakings in a directly applicable Regulation to enhance the coherence of implementation in the Member States. The PSD2 review concluded that this approach would also be appropriate in payments legislation, which has led to the proposed amendments to PSD2 being contained in two distinct legislative acts: this proposal for a Regulation containing rules for payment services providers and consumers and a proposal for a Directive containing in particular rules concerning licensing and supervision of payment institutions.

---

16 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. See also below, under "fundamental rights".

17 Directive 2019/882 of 17 April 2019 on the accessibility requirements for products and services. This is relevant for measures to improve access to SCA, which are designed to be consistent with that Directive.

18 Proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final. The Data Act proposal provides horizontal data access and use rules. Within this context and where needed, sector-specific data access rules can be adopted, including with regard to open banking rules.

19 Such as prudential rules for banks or rules on securities markets.

3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS

- **Ex-post evaluations/fitness checks of existing legislation**

An evaluation of PSD2 was carried out in 2022. Input to the evaluation included a report by an independent contractor and views of stakeholders in various public consultations. The evaluation report is published as an annex of the impact assessment accompanying the present proposal[20].

The evaluation report concludes that PSD2 has had varying degrees of success in meeting its objectives. One area of positive impact has been that of fraud prevention, via the introduction of Strong Customer Authentication (SCA); although more challenging to implement than anticipated, SCA has already had a significant impact in reducing fraud. PSD2 has also been particularly effective with regard to its goal of increasing the efficiency, transparency and choice of payment instruments for payment service users. However, there are limits to PSD2's effectiveness in achieving a level playing field, most notably given the persisting imbalance between bank and non-bank Payment Service Providers (PSPs) ensuing from the lack of direct access by the latter to certain key payment systems. There has been mixed success in the uptake of 'open banking' (OB), with issues remaining relating to data access interfaces for OB service providers, despite the costs of implementing the PSD2 provisions on OB. Regarding the internal market objective, while cross-border provision of payment services is increasing, many payment systems (especially debit card systems) remain national. Anticipated cost reductions for merchants from new and cheaper payment means have not fully materialised. Overall, the evaluation concludes that, despite certain shortcomings, the current PSD2 framework has enabled progress towards its objectives, while being relatively efficient with regard to its costs and delivering EU added value.

- **Stakeholder consultations**

To ensure that the Commission's proposal takes account of the views of all interested stakeholders, the consultation strategy for this initiative comprised:

– an open public consultation, open from 10 May 2022 to 2 August 2022[21];

– a targeted (but nevertheless public and open) consultation, with more detailed questions than the public consultation, open from 10 May 2022 to 5 July 2022[22];

– a call for evidence, open from 10 May 2022 to 02 August 2022[23];

– a targeted consultation on the SFD, open from 12 February 2021 - 7 May 2021;

– consultation of stakeholders in the Commission's Payment Systems Market Expert Group;

– ad hoc contacts with various stakeholders, either on their initiative or that of the Commission;

---

20 SWD 2023/231 final final.

21 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules/public-consultation_en

22 https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en

23 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13331-Payment-services-review-of-EU-rules_en

– Consultation of Member States' experts in the Commission Expert Group on Banking Payments and Insurance.

The outcome of these consultations is summarised in Annex 2 to the impact assessment accompanying this proposal.

- **Collection and use of expertise**

A number of inputs and sources of expertise were used in preparing this initiative, including the following:

– evidence supplied through the various consultations listed above and on an ad hoc basis by stakeholders.

– evidence provided by the European Banking Authority in its Advice[24].

– a study carried out by a contractor, Valdani Vicari & Associati Consulting, delivered in September 2022, "A study on the application and impact of Directive (EU) 2015/2366 on Payment Services (PSD2)[25].

– data obtained from private sector operators, for example in the field of open banking, and from consumer organisations.

- **Impact assessment**

These two proposals are accompanied by an impact assessment, which was examined by the Regulatory Scrutiny Board (RSB) on 1 March 2023. The RSB issued a positive opinion with reservations on 3 March 2023.

The impact assessment found that there are four key problems in the EU payment market, despite the achievements of PSD2:

– consumers are at risk of fraud and lack confidence in payments;

– the open banking framework functions imperfectly;

– EU supervisors have inconsistent powers and obligations;

– there is an unlevel playing field between banks and non-bank PSPs.

The consequences of these problems include the following:

– users (in particular consumers, merchants and SMEs) continue to be exposed to fraud risk;

– open banking service providers face obstacles to offering basic OB services and find it harder to innovate and compete with incumbent players such as cards schemes;

– PSPs experience uncertainty about their obligations, and non-bank PSPs are at a competitive disadvantage vis-à-vis banks;

– there are economic inefficiencies and higher costs of commercial operations, with negative impact on EU competitiveness;

– the internal market for payments is fragmented, with "forum shopping" occurring.

There are four specific objectives of the initiative, corresponding to the identified problems:

[24] EBA/Op/2022/06 of 23 June 2022. Contract reference FISMA/2021/OP/0002.

[25] Available at this link: https://data.europa.eu/doi/10.2874/996945.

1. Strengthen user protection and confidence in payments;
2. Improve the competitiveness of open banking services;
3. Improve enforcement and implementation in Member States;
4. Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs.

The impact assessment presents a package of preferred options, aiming to achieve the specific objectives (the list below covers both measures contained in this Regulation and in the accompanying Directive):

– For specific objective 1, improvements to the application of SCA, a legal basis for exchange of information on fraud and obligation to educate customers about fraud, extension of IBAN verification to all credit transfers, and on conditional reversal of liability for authorised push payment fraud; an obligation on PSPs to improve accessibility of SCA for users with disabilities, older people and other people facing challenges regarding the use of SCA; measures to improve the availability of cash; improvements to user rights and information.

– For specific objective 2, a requirement for account servicing PSPs (ASPSPs) to put in place a dedicated data access interface; "permissions dashboards" to allow users to manage their granted open banking access permissions; more detailed specifications of minimum requirements for OB data interfaces;

– For specific objective 3, replacing the greater part of PSD2 with a directly applicable Regulation clarifying aspects of PSD2 which are unclear or ambiguous; strengthening of provisions on penalties; integrating the licensing regimes for PIs and EMIs.

– For specific objective 4, strengthening of PI/EMI rights to a bank account; granting the possibility of direct participation of PIs and EMIs to all payment systems, including those designated by Member States pursuant to the SFD, with additional clarifications on admission and risk assessment procedures.

A number of options were rejected in the impact assessment on grounds of high implementation costs and uncertain benefits. Costs of the selected options are mainly one-off costs and fall largely on ASPSPs (essentially banks). In open banking, costs are offset by savings (such as the removal of having a permanent "fall-back" interface and of its exemption procedure) and by the adoption of proportionality measures (possible derogations for niche ASPSPs). The cost to Member States of improved enforcement and implementation will be limited. The costs of direct access to key payment systems for PIs will be limited and fall on the payment systems in question. The benefits, on the other hand, will accrue to a wide range of stakeholders, including users of payment services (consumers, businesses, merchants and public administrations) and also PSPs themselves (especially non-bank fintech PSPs). The benefits will be recurrent, while the costs will be mainly one-off adjustment costs, therefore the cumulative benefits should exceed the total costs over time.

- **Regulatory fitness and simplification**

The present initiative is not a regulatory fitness and performance programme (REFIT) initiative. Nevertheless, as part of the evaluation and review process, opportunities for administrative simplification were sought. The clarification of rules on SCA and other clarifications, together with the removal of divergences arising from national transposition of a Directive, will contribute to simplification.

- **Fundamental rights**

The fundamental right which is particularly concerned by this initiative is the protection of personal data. To the extent that processing of personal data is necessary for the compliance with this initiative, it is proportionate to ensure good functioning of the internal market for digital payments. In the context of this initiative the processing of personal data must be in line with the General Data Protection Regulation (GDPR), which applies directly to all of the payment services concerned by this proposal.

- **Application of the 'one in, one out' principle**

The present initiative does not involve administrative costs for businesses or consumers, as the initiative will not lead to any increased oversight or supervision of PSPs, or to specific new reporting obligations not already contained in PSD2. There are also no regulatory fees and charges arising from the initiative. The Commission therefore considers that this initiative does not generate administrative costs which require offsetting under the "one in one out" principle, although it is relevant for "one in one out" in that it creates implementation costs. The bringing together of the legislative regime for E-Money Institutions and that for Payment Institutions will reduce administrative costs, for example by removing the requirement to obtain a new license in certain circumstances.

- **Climate and sustainability**

No negative implications of the initiative for climate of this initiative have been identified. The initiative will contribute to target 8.2 of the UN Sustainability Development Goals: "*To achieve higher levels of economic productivity through diversification, technological upgrading and innovation, including through a focus on high-value added and labour-intensive sectors*".

4. BUDGETARY IMPLICATIONS

The present proposal has no implications for the EU budget.

5. OTHER ELEMENTS

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The initiative will provide for a review to be completed five years after the date of application. The review will have to pay particular attention to the provisions on open banking rules, fees and charges for payment services, and rules on liability and redress for fraudulent transactions.

- **Detailed explanation of the specific provisions of the proposal**

Subject matter scope and definitions

The proposal lays down rules applicable to payment services providers related to payments. It does not change the list of payment services established in PSD2. The list of exclusions is largely unchanged. There is a list of definitions, extended from the list in PSD2 and containing more terms and clarifications of certain terms. Definitions of Merchant Initiated Transactions (MITs) and of Mail Orders or Telephone Orders (MOTOs) are introduced. The definition of 'remote payment transaction' under PSD2 is streamlined to allow for a clearer delineation of 'initiation of a payment transaction' and 'remote initiation of a payment transaction'.

Payment systems and access to accounts held with credit institutions

Regarding payment system operators, the requirement to have access rules and procedures which are proportionate objective and non-discriminatory is extended also to payment systems designated by a Member State pursuant to Directive 98/26 (Settlement Finality Directive[26]). Payment system operators are required to carry out an assessment of relevant risks when considering an application for participation from a PSP. A decision on an application must be provided in writing and a right of appeal is established. Competent authorities must be designated by Member States in cases where no oversight by the European System of Central Banks exists; where there is ECSB oversight, that can be relied upon to address insufficiencies in admission rules and procedures of payment systems.

Rules concerning access (opening and closing) by a PI to an account with a credit institution are reinforced compared with PSD2. Applicants for a license as a PI (given the importance for them to have a bank account to obtain their license) are also covered, as well as PI's agents and distributors. Any refusal or withdrawal of access must be based on serious grounds, for example reasonable suspicion of illegal activity or risk to the credit institution. Reasons for refusal or withdrawal of access must be provided in writing and motivated in detail with regard to the specific situation of the PI in question.

Transparency of conditions and information requirements for payment services

Regarding the derogation from information requirements for low-value payment instruments and electronic money for national payment transactions, the option for Member States to adjust the spending limit amounts is deleted.

To ensure internal consistency, the obligation to inform the payment service user about Alternative Dispute Resolution procedures in framework contracts is extended to single payment transactions.

A clarification is included to ensure that PSPs insert in payment account statements the information needed to unambiguously identify the payee, including a reference to the payee's commercial trade name.

A clarification is included to ensure that where payment services are offered jointly with technical services supporting the provision of payment services and provided by the PSP or by a third party they have partnered with, such technical services should be subject to the framework contract requirements on termination fees.

Additional information requirements for domestic ATM withdrawals are introduced for different scenarios.

With regard to credit transfers and money remittances from the EU to a non-EU country, an obligation is introduced for PSPs to provide the payment service user with the estimated time for the funds to be received by the PSPs of the payee located outside the EU. To achieve better comparability, the estimated currency conversion charges of such international transactions must be expressed in the same way as for credit transfers within the EU, namely as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the ECB.

[26] This amendment must be considered together with a targeted amendment to the SFD contained in the accompanying proposal for a Payment Services Directive.

Rights and obligations in relation to the provision and use of payment services

Common provisions

Under PSD2, the prohibition of surcharging, covering payment services to which the Interchange Fee Regulation[27] applies, is limited under PSD2 to credit transfers and direct debits denominated in euro, and not in other currencies of the EU. Changes are introduced to extend the surcharging prohibition to credit transfers and direct debits in all currencies of the EU.

The rules for merchant initiated transactions (MITs) and direct debits are aligned, applying the same consumer protection measures, such as refunds, to direct debits and MITs as both are transactions initiated by the payee.

Open banking (account information services and payment initiation services)

The provisions on open banking contain a number of modifications compared with PSD2, and incorporate certain provisions currently contained in a Regulatory Technical Standard[28]. Key changes include the imposition, except in exceptional circumstances, of having a dedicated interface for open banking data access and the removal, except in authorised exceptional circumstances, of the requirement on account servicing PSPs to maintain permanently a 'fallback' interface. Additional requirements on dedicated interfaces are introduced as regards performance and functionalities. To enable open banking users to manage their open banking permissions in a convenient way, ASPSPs are required to offer them a "dashboard" allowing the withdrawal of data access from any given open banking provider.

There has been no significant market demand for the specific service of confirmation on the availability of funds, which was covered by article 65 of PSD2 as an open banking service alongside account information and payment initiation services. Very few, if any, business models have been developed on the basis of this service, as the market relies on the use of AIS as an alternative for checking the availability of funds. This provision has therefore been removed as a stand-alone open banking service.

Authorisation of payment transactions

The PSP of the payee is required to provide its payment service user, upon request, with a service checking that the unique identifier of the payee matches the name of the payee as provided by the payer and notifying the PSP of the payer of any detected discrepancy. Where they do not match, the PSP of the payer is to notify the payer of any such discrepancy and the detected degree thereof. The Commission proposal on instant payments amending the SEPA Regulation[29], currently in discussion by co-legislators, proposes a similar provision related to the discrepancies between the name and unique identifier of a payee for instant credit transfers denominated in euro. To achieve a coherent framework for all credit transfers, the provision in this proposal applies to credit transfers which are not instant credit transfers in all currencies of the Union and instant credit transfers in currencies which are not in euro. The notification must be given before the payer finalises the payment order and before the PSP executes the credit transfer. The user remains free to decide whether to submit the payment order for a credit transfer in all cases.

---

27 Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.

28 Commission Delegated Regulation 2018/389 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

29 Proposal COM(2022) 546 final of 26 October 2022, amending Regulation (EU) No 260/2012.

With regard to the provision on the limits for the use of a payment instrument, it is clarified that PSPs must not unilaterally increase the spending limits agreed with their payment service users.

In the provision related to the PSP's liability for unauthorised payment transactions, a clarification is added that only reasonable grounds for suspecting fraud by the payer can lead to a refusal to refund by the PSP. In such a case, the PSP must provide a justification for refusing the refund and indicate the bodies to which the payer may refer the matter.

The PSP of the payer is to be held liable for the full amount of the credit transfer in cases where that PSP has failed to notify the payer of a detected discrepancy between the unique identifier and the name of the payee provided by the payer. A PSP is held to be liable where a consumer has been manipulated into authorising a payment transaction by a third party pretending to be an employee of the consumer's PSP using lies or deception. An obligation for electronic communications services providers to cooperate with PSPs is introduced, with a view to preventing such fraud.

Where the liability is attributable to the PSP of the payee, the latter is to refund the financial damage incurred by the PSP of the payer. The provisions on notification and rectification of unauthorised or incorrectly executed payment transactions, information requirements and right of recourse are updated in order to reflect the new liability provision for incorrect application of the matching verification service.

New liability provisions for technical service providers and operators of payment schemes are included for failure to support strong customer authentication, given that the evaluation of PSD2 revealed that there were problems concerning the implementation of SCA that were linked to the roles played by such stakeholders in the roll-out of SCA, which even contributed to the postponement of the SCA application from 2018 to 2020.

A clarification is added that the payer shall not bear any financial losses where either the PSP of the payer or the payee applies an exemption from the application of strong customer authentication.

For payment transactions where the transaction amount is not known in advance and funds are blocked on a payment instrument, a legal obligation is introduced for the payee to inform the PSP of the exact amount of the payment transaction immediately after delivery of the service or goods to the payer, as well as a requirement that the amount of the blocked funds must be proportionate to the amount of the future payment transaction that can reasonably be expected at the time of blocking of the funds.

Execution of payment transactions

In cases where a payment initiation service provider provides an incorrect unique identifier of a payee, that payment initiation service provider is held to be liable for the amount of the transaction.

Data protection

A new provision is included to explicitly define substantial public interest for which the processing of special categories of personal data could be necessary in the context of this proposed Regulation.

Operational and security risks and authentication

A new provision is added requiring PSPs to have transaction monitoring mechanisms in place to provide for the application of strong customer authentication and to improve the prevention and detection of fraudulent transactions. This provision adds clarity to the notion of

‘inherence’, by detailing that such transaction monitoring mechanisms must be based on the analysis of payment transactions, taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials, including environmental and behavioural characteristics such as those related to location of the payment service user, time of transaction, device being used, spending habits, online store where the purchase is carried out.

For the purpose of transaction monitoring, provisions have been added allowing PSPs to exchange, on a voluntary basis, personal data such as unique identifiers of a payee subject to information sharing arrangements. These information sharing arrangements must define details for participation and on operational elements, including the use of dedicated IT platforms. Before concluding such arrangements, the PSPs must conduct a data protection impact assessment and, where necessary, carry out prior consultation of the supervisory authority, according to Regulation (EU) 2016/679 .

As regards the application of SCA in the case of merchant-initiated payment transactions (MITs), it is clarified that there is a need to apply strong customer authentication at the set-up of the mandate, but without any need to apply it for subsequent MITs. Regarding the application of SCA in the case of mail orders and telephone orders (MOTOs), it is clarified that only the initiation of a payment transaction needs to be non-digital in order for that transaction to not be covered by the strong customer authentication obligations. However, payment transactions based on paper-based payment orders, mail orders or telephone orders placed by the payer should be subjected to security standards and checks by the PSP of the payer allowing authentication of the payment transaction in order to prevent abusive circumvention of the strong authentication requirements. In addition, the scope of SCA exemption has been narrowed in the cases of payment transactions for which payment orders are placed by the payee based on a mandate given by the payer (direct debits), whereas an obligation to require SCA has been introduced in cases where a mandate is placed through a remote channel with the direct involvement of a payment service provider.

SCA is only required for account information services on the occasion of the first data access; however, account information service providers must require SCA when their customers access aggregated account data on the account information service provider’s domain, at least every 180 days.

Provisions have been added to improve the accessibility of SCA, in particular to ensure that all customers, including persons with disabilities, older persons, persons with low digital skills and those who do not have access to digital channels or a smartphone, have at their disposal at least one means enabling them to perform strong customer authentication.

With regard to the requirement for “remote payments” for PSPs to apply SCA that includes elements which dynamically link the transaction to a specific amount and a specific payee, it is clarified that this obligation applies to electronic payment transactions for which a payment order is placed through a payer’s device using proximity technology for the exchange of information with the payee’s infrastructure, and for which the performance of strong customer authentication requires the use of internet on the payer’s device.

There is a provision requiring payment service providers and technical service providers to enter into outsourcing agreements in cases where the latter provide and verify the elements of strong customer authentication.

Product intervention powers of the European Banking Authority

This proposal grants the EBA product intervention powers in line with Article 9(5) of Regulation 1093/2010/EU. This will allow the EBA, on the basis of some criteria, to prohibit temporarily the sale of certain payment products which would present certain risks.

Other provisions

Empowerments are provided for regulatory technical standards (RTSs) prepared by the EBA, including existing RTSs, and in certain cases, new RTSs. The EBA may amend existing RTSs but if it does not do so, they will remain in force.

The proposed Regulation will enter into force on the twentieth day after publication in the Official Journal and enter into application 18 months thereafter[30]. A correlation table of articles with respect to the corresponding articles of PSD2 and EMD2 is annexed.

[30] This date is aligned with the transposition deadline of the accompanying Payment Services Directive.

2023/0210 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on payment services in the internal market and amending Regulation (EU) No 1093/2010

(Text with EEA relevance)

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[31],

Having regard to the opinion of the European Central Bank[32],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) Since the adoption of Directive (EU) 2015/2366 of the European Parliament and of the Council[33] the retail payment services market underwent significant changes largely related to the increasing use of cards and digital means of payment, the decreasing use of cash and the growing presence of new players and services, including digital wallets and contactless payments. The Covid-19 pandemic and the transformations it brought to consumption and payment practices has increased the importance of having secure and efficient payments.

(2) The Communication from the Commission on a Retail Payments Strategy for the EU[34] announced the launch of a comprehensive review of the application and impact of Directive (EU) 2015/2366 "*which should include an overall assessment of whether it is still fit for purpose, taking into account market developments*".

(3) Directive (EU) 2015/2366 aimed at addressing barriers to new types of payment services and at improving the level of consumer protection and security. The evaluation of the impact and application of Directive (EU) 2015/2366 by the Commission found that Directive (EU) 2015/2366 has been largely successful with regard to many of its objectives, but also identified certain areas where the objectives

[31] OJ C , , p. .

[32] OJ C , , p. .

[33] 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).

[34] COM/2020/592 final.

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 margins of interpretation.

(5) Even though the issuance of electronic money is regulated under Directive 2009/110/EC of the European Parliament and of the Council[35] 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.

---

[35] 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).

(6) To ensure legal certainty and a clear scope of application of the rules applicable to the conduct of business of providing payment and electronic money services, it is necessary to specify the categories of payment service providers which are subject to the obligations concerning the conduct of the business of providing payment services and electronic money services throughout the Union.

(7) There are several categories of payment service providers. Credit institutions take deposits from users that can be used to execute payment transactions. They are authorised pursuant to Directive 2013/36/EU of the European Parliament and of the Council[36]. Payment institutions don't take deposits. They may hold users funds and issue electronic money that can be used to execute payment transactions. They are authorised pursuant to Directive (EU) XXX [PSD3]. Post office giro institutions which are entitled to do so under national law may 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.

(8) It is appropriate to dissociate the service of enabling cash to be withdrawn from a payment account from the activity of servicing a payment account, as the providers of cash withdrawal services may not service payment accounts. The services of issuing payment instruments and of acquiring payment transactions, which were listed together in point 5 of the Annex to Directive (EU) 2015/2366 as if one could not be offered without the other, should be presented as two different payment services. Listing issuing and acquiring services separately should, together with distinct definitions of each service, clarify that the issuing and acquiring services may be offered separately by payment service providers.

(9) The exclusion from the scope of Directive (EU) 2015/2366 of certain categories of operators of automated teller machines (ATM) has proven difficult to apply in practice. Therefore, the category of ATM operators which were excluded from the requirement to be authorised as a payment service provider under Directive (EU) 2015/2366 should be replaced by a new category of ATM operators which do not service payment accounts. While those operators are not subject to the authorisation requirements under Directive (EU) XXX [PSD3], they should however be subject to requirements on fees transparency in situations where such ATM operators levy charges for cash withdrawals.

(10) To further improve access to cash, which is a priority of the Commission, merchants should be allowed to offer, in physical shops, cash provision services even in the absence of a purchase by a customer, without having to obtain a payment service provider authorisation or being an agent of a payment institution. Those cash provision services should, however, be subject to the obligation to disclose fees charged to the customer, if any. These services should be provided by retailers on a voluntary basis and should depend on the availability of cash by the retailer.

(11) The exclusion from the scope of Directive (EU) 2015/2366 of payment transactions from the payer to the payee through a commercial agent acting on behalf of the payer

[36] 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).

or the payee has been applied very differently across Member States. The concept of commercial agents is typically defined in national civil law, which might diverge form Member State to Member State, leading to inconsistent treatment of the same services in different jurisdictions. The concept of commercial agents under that exclusion should therefore be harmonised and clarified by making reference to the definition of commercial agents as laid down in Council Directive 86/653/EEC[37]. In addition, further clarity should be provided on the conditions under which payment transactions from the payer to the payee through commercial agents may be excluded from the scope of this Regulation. This is achieved by requiring that agents should be authorised via an agreement with either the payer or the payee to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee, but not both of them, regardless of whether or not the commercial agent is in the possession of client's funds. Electronic commerce platforms that act as commercial agents on behalf of both individual buyers and sellers without buyers or sellers having any real margin or autonomy to negotiate or to conclude the sale or purchase of goods or services should not be excluded from the scope of this Regulation. The European Banking Authority (EBA) should develop guidelines on the exclusion for payment transactions from the payer to the payee through a commercial agent to provide further clarity and convergence among competent authorities. Those guidelines may include a repository of use cases typically covered by the commercial agent exclusion.

(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[38]. 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.

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

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

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

childcare vouchers or ecological vouchers. Specific-purpose instruments should also include electronic money-based instruments once they meet the requirements of this exclusion. Payment instruments which can be used for purchases in stores of listed merchants should not be excluded, as such instruments are typically designed for a network of service providers which is continuously growing.

(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 to so that customers can still easily order, pay for, obtain and validate electronic tickets from any location and at any time using mobile phones or other devices. Electronic tickets allow and facilitate the delivery of services that consumers could otherwise purchase in paper ticket form and include transport, entertainment, car parking and entry to venues, but exclude physical goods. Payment transactions by a specified provider of electronic communications networks performed from or via an electronic device and charged to the related bill to collect charitable donations should also be excluded. It should apply only where the value of payment transactions is below a specified threshold.

(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 between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking which are provided by a payment service provider belonging to the same group should be excluded from the scope of this Regulation. The collection of payment orders on behalf of a group by a parent undertaking or its subsidiary for onward transmission to another payment service provider should not be considered as a payment service.

(16) The provision of payment services requires the support of technical services. Those technical services include the processing and storage of data, payment gateway services, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of consumer-facing interfaces used to collect payment information, including terminals and devices used for payment services. Payment initiation services and account information services are not technical services.

(17) Technical services do not constitute payment services as such as technical service providers do not enter at any time into possession of the funds to be transferred. They should therefore be excluded from the definition of payment services. Those services should however be subject to certain requirements, such as those on liability for failure to support the application of strong customer authentication, or the requirement to enter into outsourcing agreements with payment service providers in case technical service providers are to provide and verify the elements of strong customer authentication. There should also be requirements governing the termination fees of framework contracts where payment services are offered jointly with technical services.

(18) Taking into account the rapid evolution of the retail payments market and the emergence of new payment services and payment solutions, it is appropriate to adapt some of the definitions under Directive (EU) 2015/2366 to the realities of the market in order to ensure that Union legislation remains fit for purpose and technology neutral.

(19) The clarification of the process and the various steps to be followed for the execution of a payment transaction is of significant importance for the rights and obligations of the parties involved in a payment transaction and for the application of strong customer authentication. The process leading to the execution of a payment transaction is either initiated by the payer or on his/her behalf, or by the payee. The payer initiates the payment transaction by placing a payment order. Once the payment order is placed, the payment service provider checks if the transaction has been authorised and authenticated including, where applicable, by applying strong customer authentication, and the payment service provider then validates the payment order. The payment service provider then takes the relevant steps to execute the payment transaction, including the transfer of funds.

(20) Given the diverging views identified by the Commission in it its review of the implementation of Directive (EU) 2015/2366 and highlighted by the European Banking Authority (EBA) in its opinion of 23 June 2022 on the review of Directive (EU) 2015/2366, it is necessary to clarify the definition of a payment accounts. The determining criterion for the categorisation of an account as payment account lies in the ability to perform daily payment transactions from such an account. The possibility of making payment transactions to a third party from an account or of benefiting from such transactions carried out by a third party is a defining feature of the concept of payment account. A payment account should therefore be defined as an account that is used for sending and receiving funds to and from third parties. Any account that possesses those characteristics should be considered a payment account and should be accessed for the provision of payment initiation and account information services. Situations where another intermediary account is needed to execute payment transactions from or to third parties should not fall under the definition of a payment account. Savings accounts are not used for sending and receiving funds to or from a third party, excluding them therefore from the definition of a payment account.

(21) Given the emergence of new types of payment instruments and the uncertainties prevailing in the market as to their legal qualification, the definition of a ‘payment instrument’ should be further specified by providing some examples to illustrate what constitutes or does not constitute a payment instrument, bearing in mind the principle of technology neutrality.

(22) Despite the fact that Near-Field Communication (NFC) enables the initiation of a payment transaction, considering it as a fully-fledged ‘payment instrument’ would pose some challenges, for example for the application of strong customer authentication for contactless payments at the point of sale and of the payment service provider’s liability regime. NFC should therefore rather be considered as a functionality of a payment instrument and not as a payment instrument as such.

(23) The definition of ‘payment instrument’ under Directive (EU) 2015/2366 referred to a ‘personalised device’. Since there are pre-paid cards where the name of the holder of the instrument is not printed on the card, applying that reference could leave those types of cards outside the scope of the definition of a payment instrument. The definition of ‘payment instrument’ should, therefore, be amended to refer to ‘individualised’ devices instead of ‘personalised’ ones, clarifying that pre-paid cards where the name of the holder of the instrument is not printed on the card fall within the scope of this Regulation.

(24) So-called digital 'pass-through wallets', involving the tokenisation of an existing payment instrument, for example a payment card, are to be considered as technical services and should thus be excluded from the definition of payment instrument as, in the Commission's view, a token cannot be regarded as being itself a payment instrument but, rather, a 'payment application' within the meaning of Article 2(21) of Regulation (EU) 2015/751 of the European Parliament and of the Council.[39] However, some other categories of digital wallets, namely pre-paid electronic wallets such as 'staged-wallets' where users can store money for future online transactions, should be considered a payment instrument and their issuance a payment service.

(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 permission to access and aggregate the data, but to another party, to enable it to provide other services to the consumer using the data. There are however diverging views as to whether this activity falls under the regulated account information service. The Commission considers that this 'license-as-a-service' evolution of the 'open banking' business model can be a source of innovative, data-based services, to the ultimate benefit of end-users. Indeed, that business model enables end-users to give access to their payment account data in order to receive other - non-payment - services including lending, accounting, creditworthiness assessment. It is however essential that payment service users know precisely who accesses their payment account data, on what legal grounds and for what purpose. Payment service users should be made fully aware of and authorise the transmission of their data to another company. That new open banking-based business model requires a modification of the definition of account information services, to clarify that the information aggregated by the authorised account information service provider may be transmitted to a third party to enable that third party to provide another service to the end-user, with the end-user's permission. To provide consumers with adequate protection for their payment account data and legal certainty about the status of entities accessing their data, the service of data aggregation from payment accounts should always be provided by a regulated entity on the basis of a license, even where the data is ultimately transmitted to another service provider.

(27) Money remittance is a payment service that is usually based on cash provided by a payer to a payment service provider, without any payment accounts being created in the name of the payer or the payee, which remits the corresponding amount to a payee or to another payment service provider acting on behalf of the payee. In some Member States, supermarkets, merchants and other retailers provide to the public a service enabling the public to pay utilities and other regular household bills. Those bill-paying services should be treated as money remittance.

---

[39] 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).

(28) The definition of funds should cover all forms of central bank money issued for retail use, including banknotes and coins, and any possible future central bank digital currency, e-money and commercial bank money. Central bank money issued for use between the central bank and commercial banks, i.e. for wholesale use, should not be covered.

(29) Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets lays down that electronic-money tokens shall be deemed to be electronic money. Electronic money tokens are therefore included, as electronic money, in the definition of funds in this Regulation.

(30) To preserve the confidence of the electronic money holder, electronic money needs to be redeemable. Redeemability does not imply that the funds received in exchange for electronic money should be regarded as deposits or other repayable funds for the purpose of Directive 2013/36/EU[40]. 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.

(31) Payment service providers need access to payment systems to provide payment services to users. Those payment systems typically include four-party card schemes as well as major systems processing credit transfers and direct debits. To ensure equality of treatment throughout the Union between the different categories of authorised payment service providers it is necessary to clarify the rules concerning access to payment systems. Such access may be direct or indirect via another participant in that payment system. Such access should be subject to requirements that ensure integrity and stability of those payment systems. To that end the payment system operator should carry out a risk assessment of a payment service provider which applies for direct participation; that risk assessment should examine all relevant risks, including where applicable settlement risk, operational risk, credit risk, liquidity risk and business risk. Each payment service provider applying for participation in a payment system should bear the risk of its own choice of system and provide proof to the payment system that its internal arrangements are sufficiently robust against those types of risk. Payment system operators should only reject an application for direct participation by a payment service provider if the payment service provider is unable to respect the rules of the system or poses an unacceptably high level of risk.

(32) Payment system operators should have in place rules and procedures on access which are proportionate objective non-discriminatory and transparent. Payment system operators should not discriminate against payment institutions as regards participation if the system rules can be respected and there is no unacceptable risk to the system. Such systems include, amongst others, those designated under Directive 98/26/EC of

[40] 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).

the European Parliament and of the Council[41]. In cases where the payment system in question is already subject to oversight by the European System of Central Banks under Regulation of the European Central Bank (EU) No 795/2014[42], the central bank or banks exercising that oversight should monitor respect of those rules in the framework of their oversight. In cases of other payment systems, Member States should designate national competent authorities to ensure that payment system infrastructure operators respect such requirements.

(33) To ensure fair competition between payment service providers, a participant in a payment system which provides services in relation to such a system to an authorised or registered payment service provider should also, when requested to do so, grant access to such services in an objective, proportionate and non-discriminatory manner to any other authorised or registered payment service provider.

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

(35) Payment institutions need to be able to open and maintain an account with a credit institution to meet their licensing requirements as regards safeguarding of customer funds. However, as evidenced in particular by the EBA in its Opinion of 5 January 2022,[43] despite the provisions on payment institution accounts with a commercial bank laid down in Directive (EU) 2015/2366, some payment institutions or companies applying for a payment institution license still face practices from some credit institutions which either refuse to open an account for them or close an account where one exists, based on perceived higher risk of money laundering or terrorism financing. Those so-called ‘de-risking’ practices create significant competitive challenges for payment institutions.

(36) Credit institutions should therefore provide a payment account to payment institutions, and to applicants for a license as a payment institution, as well as to their agents and distributors, except in exceptional cases where there are serious grounds to refuse access. It is necessary to include applicants for a license as a payment institution in that provision, given the fact that a bank account where clients’ funds can be safeguarded is a prerequisite to obtain a payment institution license. The grounds for

---

[41] 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).

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

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

refusal should include serious grounds for suspicion of illegal activities being pursued by or via the payment institution, or a business model or risk profile which causes serious risks or excessive compliance costs for the credit institution. For instance, business models where payment institutions use a vast network of agents may generate significant anti-money laundering and combating the financing of terrorism (AML/CFT) compliance costs. A payment institution should have the right of appeal against a refusal by a credit institution to a competent authority designated by a Member State. In order to facilitate the exercise of that appeal right, credit institutions should motivate in writing and in detail any refusal to provide an account, or a subsequent closure of an account. That motivation should refer to specific elements relating to the payment institution in question, not to general or generic considerations. To facilitate treatment by competent authorities of appeals against account refusal or withdrawal and motivation thereof, the EBA should develop implementing technical standards harmonising the presentation of such motivations.

(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 and clear information about payment services. To ensure that necessary, sufficient and comprehensible information is given to payment service users with regard to the payment service contract and payment transactions, it is necessary to specify and to harmonise the obligations on payment service providers as regards the provision of information to payment service users.

(38) When providing the required information to payment service users, payment service providers should take into account the needs of payment service users and practical aspects and cost-efficiency depending on the respective payment service contract. Payment service providers should either actively communicate at the appropriate time without any prompting by the payment service user, or they should make the information available to payment service users request. In the second situation, payment service users should take active steps to obtain the information, including requesting that information explicitly from payment service providers, logging into a bank account mailbox or inserting a bank card into a printer for account statements. For those purposes, the payment service providers should ensure that access to the information is possible, and that the information is available to payment service users.

(39) As consumers and undertakings are not in the same position of vulnerability, they do not need the same level of protection. While it is important to guarantee consumer rights by provisions from which it is not possible to derogate by contract, it is reasonable to let undertakings and organisations agree otherwise when they are not dealing with consumers. Micro-enterprises, as defined in Commission Recommendation 2003/361/EC,[44] may be treated in the same way as consumers. Certain rules should always apply, irrespective of the status of the user.

(40) To maintain a high level of consumer protection, consumers should have the right to receive information on services conditions and prices free of charge before being bound by any payment service contract. To enable consumers to compare the services and conditions offered by payment service providers and, in the case of a dispute, to verify their contractual rights and obligations, consumers should be able to request that information and the framework contract on paper, free of charge and at any time during the contractual relationship.

---

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

(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 all applicable charges for domestic ATM withdrawals in different situations, depending on the ATM from which the payment service users withdraw cash.

(46) Framework contracts and the payment transactions covered by those contracts are more common and economically significant than single payment transactions. If there is a payment account or a specific payment instrument, a framework contract is required. Therefore, the requirements for prior information on framework contracts should be comprehensive and information should always be provided on paper or on another durable medium. However, payment service providers and payment service users should be able to agree in the framework contract on the manner in which subsequent information on executed payment transactions is to be given.

(47) Contractual provisions should not discriminate against consumers who are legally resident in the Union on the grounds of their nationality or place of residence. Where a framework contract provides for the right to block a payment instrument for objectively justified reasons, the payment service provider should not be able to

invoke that right merely because the payment service user has changed his or her place of residence within the Union.

(48) To ensure a high level of consumer protection, Member States should, in the interest of the consumer, be able to maintain or introduce restrictions or prohibitions on unilateral changes in the conditions of a framework contract, for instance if there is no justified reason for such a change.

(49) To facilitate payment service users' mobility, users should be able to terminate a framework contract without incurring charges. However, for contracts terminated by the payment service users less than 6 months after their entry into force, payment service providers should be allowed to apply charges in line with the costs incurred due to the termination of the framework contract by the user. Where, under a framework contract, payment services are offered jointly with technical services supporting the provision of payment services, such as the rental of terminals used for payment services, payment service users should not be locked in with their payment service provider via more onerous terms set in the contractual clauses governing the technical services. To preserve competition, such contractual terms should be subject to the framework contract requirements on termination fees. For consumers, the period of notice agreed should be no longer than 1 month, and for payment service providers no shorter than 2 months. Those rules should be without prejudice to the payment service provider's obligation to terminate the payment service contract in exceptional circumstances under other relevant Union or national law, such as that on money laundering or financing of terrorism, any action targeting the freezing of funds, or any specific measure linked to the prevention and investigation of crimes.

(50) To achieve comparability, the estimated currency conversion charges for credit transfers and remittances carried out within the Union and from the Union to a third country should be expressed in the same way, namely as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the European Central Bank (ECB). When reference is made to 'charges' in this Regulation, it should also cover, where applicable, 'currency conversion' charges.

(51) Experience has shown that the sharing of charges between a payer and a payee is the most efficient system since it facilitates the straight-through processing of payments. Provision should therefore be made for charges to be levied directly on the payer and the payee by their respective payment service providers. The amount of any charges levied may also be zero as the rules should not affect the practice whereby a payment service provider does not charge consumers for crediting their accounts. Similarly, depending on the contract terms, a payment service provider may charge only the payee for the use of the payment service, in which case no charges are imposed on the payer. It is possible that the payment systems impose charges by way of a subscription fee. The provisions on the amount transferred or any charges levied have no direct impact on pricing between payment service providers or any intermediaries.

(52) A surcharge is a charge by merchants to consumers that is added on top of the requested price for goods and services when a certain payment method is used by the consumer. One of the reasons for surcharging is to direct consumers to cheaper or more efficient payment instruments, hence fostering competition between alternative payment methods. Under the regime introduced by Directive (EU) 2015/2366, payees were prevented from requesting charges for the use of payment instruments for which interchange fees are regulated under Chapter II of Regulation (EU) 2015/751, i.e. for consumer debit and credit cards issued under four-party card schemes, and for those

payment services to which Regulation (EU) No 260/2012 of the European Parliament and of the Council[45] applies, i.e. credit transfer and direct debit transactions denominated in euro within the Union. Member States were allowed under Directive (EU) 2015/2366 to further prohibit or limit the right of the payee to request charges, taking into account the need to encourage competition and promote the use of efficient payment instruments.

(53) Evidence gathered during the review of Directive (EU) 2015/2366 shows that the current rules on charges are appropriate and had a positive impact. There is no compelling need for further alignment of charging practices between Member States, as the existing surcharging ban already applies to a very large share of payments in the Union. It is estimated that 95% of card payments are subject to the existing surcharging ban. In addition, when a surcharge is applied, it is capped at the actual cost incurred by the merchant. However, in its review of Directive (EU) 2015/2366, the Commission identified different interpretations concerning the payment instruments covered by the surcharging ban. It is therefore necessary to explicitly extend the surcharging ban to all credit transfers and direct debits and not just to those covered by Regulation (EU) No 260/2012, as was the case under Directive (EU) 2015/2366.

(54) Account information services and payment initiation services, often collectively known as 'open banking services', are payment services involving access to the data of a payment service user by payment service providers which do not hold the account holder's funds nor service a payment account. Account information services allow the aggregation of a user's data, at the request of the payment service user, with different account servicing payment service providers in one single place. Payment initiation services allow the initiation of a payment from the user's account, such as a credit transfer or a direct debit, in a convenient way for the user and the payee without the use of an instrument such as a payment card.

(55) Account servicing payment service providers should allow access by account information and payment initiation service providers to payment account data if the payment account can be accessed by the payment service user online and if the payment service user has granted permission for such access. Directive (EU) 2015/2366 was based on the principle of access to payment account data without a need for a contractual relationship between the account servicing payment service provider and the account information and payment initiation service providers, which had the effect that charging for access to data was in practice not possible. Access to data under open banking has been taking place on such a non-contractual basis, and without charging, since the application of Directive (EU) 2015/2366. If regulated data access services were to be subjected to a charge, where there was no charge hitherto, the impact on the continued provision of those services, and therefore on competition and innovation in payment markets, could be very significant. That principle should therefore be maintained. Maintaining that approach is in line with Chapters III and IV of the proposal of a Regulation on harmonised rules on fair access to and use of data (Data Act)[46], in particular Article 9(3) of that proposal on compensation, to which this

---

45 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).

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

Regulation is without prejudice. The Commission's proposal for a Regulation on Financial Data Access (FIDA) provides for a possible compensation for data access which will be covered by FIDA. Such regime would thus be different from the one governed by the present Regulation. This difference of treatment is justified by the fact that, unlike for payment account data access, which is regulated by Union law since the entry into force of Directive (EU) 2015/2366, access to other financial data has not yet been subject to Union regulation. There is therefore no risk of disruption as, unlike access to payment account data, this market is emerging and will be regulated for the first time with FIDA.

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

(57) To guarantee a high level of security in data access and exchange, access to payment accounts and the data therein should, barring specific circumstances, be provided to account information and payment initiation service providers via an interface designed and dedicated for 'open banking' purposes, such as an API. To that end, the account servicing payment service provider should set up a secure communication with account information and payment initiation service providers. To avoid any uncertainty as to who is accessing the payment service user's data, the dedicated interface should enable account information and payment initiation service providers to identify themselves to the account servicing payment service provider, and to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user. Account information and payment initiation service providers should as a general rule use the interface dedicated for their access and therefore should not use the customer interface of an account servicing payment service provider for the purpose of data access, except in cases of failure or unavailability of the dedicated interface in the conditions laid down in this Regulation. In such circumstances their business continuity would be endangered by their incapacity to access the data for which they have been granted a permission. It is indispensable that account information and payment initiation service providers be at all times able to access the data indispensable for them to service their clients.

(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).

(59) For account information and payment initiation service providers to ensure at all times their business continuity and to be able to provide high quality services to their clients, the dedicated interface that they are expected to use must meet high level requirements in terms of performance and functionalities. It should at a minimum ensure 'data parity' with the customer interface provided to its users by the account servicing payment service provider, therefore including the payment account data which is also available to the payment service users in the interface provided to them by the account servicing payment service provider. With regard to payment initiation services, the dedicated interface should allow not only the initiation of single payments but of standing orders and direct debits. More detailed requirements for dedicated interfaces should be laid down in Regulatory Technical Standards developed by the EBA.

(60) Given the dramatic impact that a prolonged unavailability of a dedicated interface would have on account information and payment initiation service providers' business continuity, account servicing payment service providers should remedy such unavailability without delay. Account servicing payment service providers should inform account information and payment initiation service providers of any such unavailability of their dedicated interface and of the measures taken to remedy them without delay. In case of unavailability of a dedicated interface, and where no effective alternative solution is offered by the account servicing payment service provider, account information and payment initiation service providers should be able to preserve their business continuity. They should be allowed to request their national competent authority to make use of the interface provided to its users by the account servicing payment service provider until the dedicated interface is again available. The competent authority should, upon receiving the request, take its decision without delay. Pending the decision from the authority the requesting account information and payment initiation service providers should be allowed to temporarily use the interface provided to its users by the account servicing payment service provider. The relevant competent authority should set a deadline to the account servicing payment service provider to restore the full functioning of the dedicated interface, with the possibility of sanctions in case of failure to do so by the deadline. All account information and payment initiation service providers, not just those which introduced the request, should be allowed to access the data they need to ensure their business continuity.

(61) Such temporary direct access should have no negative effect on consumers. Account information and payment initiation service providers should therefore always duly identify themselves and respect all their obligations, such as the limits of the permission which was granted to them, and should in particular access only the data that they need to meet their contractual obligations and provide the regulated service. Access to payments account data without proper identification (so-called 'screen-scraping') should, in any circumstances, never be performed.

(62) Given the fact that setting up a dedicated interface could, for certain account servicing payment service providers, be deemed disproportionately burdensome, a national

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

(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. Sometimes more information becomes available to the account servicing payment service provider after it has received the payment order, but before it has executed the payment transaction. Where relevant for the payment order and the execution of the payment transaction, the account servicing payment service provider should provide that information to the payment initiation service provider. The payment initiation service provider should benefit from the information necessary to assess the risks of non-execution of the initiated transaction. That information is indispensable to enable the payment initiation service provider to offer to a payee on behalf of whom it initiates the transaction a service whose quality can compete with other means of electronic payments available to the payee, including payment cards.

(65) To increase trust in open banking, it is essential that payment service users who use account information and payment initiation services be in full control of their data and have access to clear information on the data access permissions that those payment service users have granted to payment service providers, including the purpose of permission and the categories of payment account data concerned, including identity data of the account, transaction and account balance. Account servicing payment service providers should therefore make available to payment service users who use such services a 'dashboard', for monitoring and withdrawing or re-establishing data access granted to 'open banking' services providers. Permissions for initiation of one-off payments should not feature on that dashboard. A dashboard may not allow a payment service user to establish new data access permissions with an account information or payment initiation service provider to which no previous data access has been given. Account servicing payment service providers should inform account information and payment initiation service providers promptly of any withdrawal of

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

(66) The review of Directive (EU) 2015/2366 has revealed that account information and payment initiation service providers are still exposed to many unjustified obstacles, despite the level of harmonisation achieved and of the prohibition on such obstacles imposed by Article 32(3) of Commission Delegated Regulation (EU) 2018/389[47]. Those obstacles still significantly hamper the full potential of open banking in the Union. Those obstacles are regularly reported by account information and payment initiation service providers to supervisors, regulators and the Commission. They were analysed by the EBA in its June 2020 Opinion on "*Obstacles to the provision of third-party provider services under the Payment Services Directive*". Despite clarifications efforts made there is still a lot of uncertainty, in the market and with supervisors, as to what constitutes a 'prohibited obstacle' to regulated open banking services. It is therefore indispensable to provide a clear and non-exhaustive list of such prohibited open banking obstacles, relying in particular on the work carried out by the EBA.

(67) The obligation to keep personalised security credentials safe is of the utmost importance to protect the funds of the payment service user and to limit the risks relating to fraud and unauthorised access to payment accounts. However, terms and conditions or other obligations imposed by payment service providers on payment service users in relation to keeping personalised security credentials safe should not be drafted in a way that prevents payment service users from taking advantage of services offered by other payment service providers, including payment initiation services and account information services. Such terms and conditions should not contain any provisions that would make it more difficult, in any way, to use the payment services of other payment service providers authorised or registered pursuant to Directive (EU) XXX (PSD3). Furthermore, it is appropriate to specify that, for the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data.

---

[47] 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).

(68) To be fully successful, 'open banking' requires a robust and effective enforcement of the rules that regulate that activity. As there exists no single authority at the level of the Union to enforce 'open banking' rights and duties, national competent authorities are the first level of open banking enforcement. It is essential that national competent authorities proactively and rigorously ensure the respect of the Union 'open banking' regulated framework. Insufficient enforcement by the relevant authorities is regularly presented by open banking operators as being one of the reasons for its still limited take-up in the Union. National competent authorities should have the appropriate resources to perform their enforcement tasks effectively and efficiently. National competent authorities should promote and broker a smooth and regular dialogue between the various actors of the 'open banking' ecosystem. Account servicing payment service providers and account information and payment initiation service providers which do not comply with their obligations should be subjected to appropriate sanctions. Regular monitoring of the 'open banking' market in the Union by competent authorities, coordinated by the EBA, should facilitate enforcement, and collection of data on the 'open banking' market will remedy a data gap which currently exists, hampering any effective measurement of the actual take-up of 'open banking' in the Union. Account servicing payment service providers and account information and payment initiation service providers should have access to dispute settlement bodies, pursuant to Article 10 of the Data Act proposal, once that Regulation enters into force.

(69) The parallel use of the term 'explicit consent' in Directive (EU) 2015/2366 and Regulation (EU) 2016/679 of the European Parliament and of the Council[48] has led to misinterpretations. The object of the explicit consent under Article 94 (2) of Directive (EU) 2015/2366 is the permission to obtain access to those personal data, to be able to process and store these personal data that are necessary for the purpose of providing the payment service. Therefore, a clarification should be made to increase legal certainty and have a clear differentiation with data protection rules. Where the term 'explicit consent' was used in Directive (EU) 2015/2366, the term 'permission' should be used in the present Regulation. When reference is made to 'permission' that reference should be without prejudice to obligations of payment service providers under Article 6 of Regulation (EU) 2016/679. Therefore, permission should not be construed exclusively as 'consent' or 'explicit consent' as defined in Regulation (EU) 2016/679.

(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 would verify whether there is any discrepancy between the unique identifier of the payee and the name of the payee provided by the payer and, should any such discrepancies be detected, notify the payer thereof. Such services, in the countries where they exist, have had a substantial positive impact on the level of fraud and errors. Given the importance of that service for the prevention of fraud and errors,

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

such service should be available free of charge to consumers. To avoid undue frictions or delays in the processing of the transaction, the payment service provider of the payer should provide such notification within no more than a few seconds from the moment the payer has entered the payee information. To enable the payer to decide whether to proceed with the intended transaction, the payment service provider of the payer should provide such notification before the payer authorises the transaction. Certain credit transfer initiation solutions may be available to payers allowing them to place a payment order without inserting themselves the unique identifier. Instead, such data elements are provided by the provider of that initiation solution. In such cases, there is no need for a service verifying the match between the unique identifier and the name of the payee since the risk of fraud or errors is significantly reduced.

(71) Regulation (EU) XXX amending Regulation (EU) No 260/2012 provides for a service verifying the match between the unique identifier and the name of the payee to be offered to users of instant credit transfers in euro. To achieve a coherent framework for all credit transfers whilst avoiding any undue overlap, the verification service referred to in the present Regulation should only apply to credit transfers which are not covered by Regulation (EU) XXX amending Regulation (EU) No 260/2012.

(72) Some attributes of the name of the payee to whose account the payer wishes to make a credit transfer may increase the likelihood of a discrepancy being detected by the payment service provider, including the presence of diacritics or different possible transliterations of names in different alphabets, differences between habitually used names and names indicated on formal identification documents in case of natural persons, or differences between commercial and legal names in case of legal persons. To avoid undue frictions in the processing of credit transfers and facilitate the payer's decision on whether to proceed with the intended transaction, payment service providers should indicate the degree of such discrepancy by indicating in the notification where there is no match or a 'close' match.

(73) Authorising a payment transaction despite the matching verification service having detected a discrepancy and notified that discrepancy to the payment service user can result in the funds being transferred to an unintended payee. Payment service providers should inform payment service users about the possible consequences of their choice to ignore the notified discrepancy and proceed with the execution of the transaction. Payment service users should be able to opt out from using such a service at any time during their contractual relationship with the payment service provider. After opting out, payment service users should be able to avail again of the service.

(74) The payment service user should inform the payment service provider as soon as possible about any contestations concerning allegedly unauthorised, incorrectly executed payment transactions or authorised credit transfers where there was a malfunctioning of the matching verification service, provided that the payment service provider has fulfilled its information obligations. If the notification deadline has been met by the payment service user, the payment service user should be able to pursue those claims subject to national limitation periods. That should not affect other claims between payment service users and payment service providers.

(75) Provision should be made for the allocation of losses in the case of unauthorised payment transactions or of specific authorised credit transfers. Different provisions may apply to payment service users who are not consumers, since such users are normally in a better position to assess the risk of fraud and take countervailing measures. To ensure a high level of consumer protection, payers should always be

entitled to address their claim to a refund to their account servicing payment service provider, even where a payment initiation service provider is involved in the payment transaction. That should be without prejudice to the allocation of liability between the payment service providers.

(76) In the case of payment initiation services, the allocation of liability between the payment service provider servicing the account and the payment initiation service provider involved in the transaction should compel them to take responsibility for the respective parts of the transaction that are under their control.

(77) In the case of an unauthorised payment transaction, the payment service provider should immediately refund the amount of that transaction to the payer. However, where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payer and where that suspicion is based on objective grounds which are communicated to the relevant national authority by the payment service provider, the payment service provider should be able to conduct an investigation before refunding the payer. The payment service provider should, within 10 business days after noting or being notified of the transaction, either refund the payer the amount of the unauthorised payment transaction or provide the payer the reasons and supporting evidence for refusing the refund and indicate the bodies to which the payer may refer the matter if the payer does not accept the reasons provided. To protect the payer from any disadvantages, the credit value date of the refund should not be later than the date when the amount was debited. To provide an incentive for the payment service user to notify, without undue delay, the payment service provider of any theft or loss of a payment instrument and thus to reduce the risk of unauthorised payment transactions, the user should be liable only for a very limited amount unless the payment service user has acted fraudulently or with gross negligence. In that context, an amount of EUR 50 seems to be adequate in order to ensure a harmonised and high-level user protection within the Union. There should be no liability where the payer is not able to become aware of the loss, theft or misappropriation of the payment instrument. Moreover, once a payment service user has notified a payment service provider that his or her payment instrument may have been compromised, the payment service user should not be required to cover any further losses stemming from unauthorised use of that instrument. Payment service providers should be responsible for the technical security of their own products.

(78) Liability provisions in the case of authorised credit transfers where there was an incorrect application or malfunctioning of the service detecting discrepancies between the name and unique identifier of a payee would create the right incentives for payment service providers to provide a fully functioning service, with the aim of reducing the risk of ill-informed payment authorisations. If the payer decided to make use of such a service, the payment service provider of the payer should be held liable for the full amount of the credit transfer in cases where that payment service provider failed, whereas it should have done so if properly functioning, to notify the payer of a discrepancy between the unique identifier and the name of the payee provided by the payer and such failure caused a financial damage to the payer. Where the liability of the payment service provider of the payer is attributable to the payment service provider of the payee, the payment service provider of the payee should compensate the payment service provider of the payer for the financial damage incurred.

(79) Consumers should be adequately protected in the context of certain fraudulent payment transactions that they have authorised without knowing these transactions were fraudulent. The number of ‘social engineering’ cases where consumers are

misled into authorising a payment transaction to a fraudster has significantly increased in recent years. 'Spoofing' cases where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name, mail address or telephone number to gain the customers' trust and trick them into carrying-out some actions, are unfortunately becoming more widespread in the Union. Those new types of 'spoofing' fraud are blurring the difference that existed in Directive (EU) 2015/2366 between authorised and unauthorised transactions. Means through which the consent may be assumed to be granted are also becoming more complex to identify, as fraudsters can take control of the whole consent and authentication process including of the strong customer authentication completion. The conditions under which the customer authorised a transaction by giving his or her permission to it should be taken into due consideration, including by courts, to qualify a transaction as being authorised or unauthorised. A transaction may indeed have been authorised in circumstances where such authorisation was granted on manipulated premises affecting the integrity of the permission. It is therefore no longer possible, as was the case in Directive (EU) 2015/2366, to limit refunds to unauthorised transactions only. It would however be disproportionate and financially very costly to payment services providers to open every fraudulent transaction, authorised or unauthorised, to a systematic refund right. It might also cause moral hazard and a reduction in the customer's vigilance.

(80) Payment service providers could be also considered as victims of 'spoofing' cases, as their details were usurped. However, payment service providers have more means than consumers to put an end to these fraud cases, through adequate prevention and robust technical safeguards developed with electronic communications services providers such as mobile network operators, internet platforms etc. Cases of bank employee impersonation fraud affect the good repute of the bank, of the banking sector as a whole and may cause significant financial damages to Union consumers, affecting their trust in electronic payments and in the banking system. A good-faith consumer who has been the victim of such 'spoofing' fraud where fraudsters pretend to be employees of a customer's payment service provider and misuse the payment service provider's name, mail address or telephone number should therefore be entitled to a refund of the full amount of the fraudulent payment transaction from the payment service provider, unless the payer has acted fraudulently or with 'gross negligence'. As soon as the consumer becomes aware that he or she has been a victim of that type of spoofing fraud, the consumer should without undue delay report the incident to the police, preferably via online complaint procedures, where made available by the police, and to his or her payment service provider, providing every necessary supporting evidence. No refund should be granted where those procedural conditions are not fulfilled.

(81) Given their obligations to safeguard the security of their services in accordance with Directive 2002/58/EC of the European Parliament and of the Council[49], electronic communications services providers have the capacity to contribute to the collective fight against 'spoofing' fraud. Therefore, and without prejudice to the obligations laid down in national law implementing that Directive, electronic communications services providers should cooperate with payment service providers with a view to preventing

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

further occurrences of that type of fraud, including by acting promptly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC. Any claim by a payment service provider against other providers, such as electronic communications services providers, for financial damage caused in the context of this type of fraud should be made in accordance with national law.

(82) To assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, 'gross negligence' should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. The fact that a consumer has already received a refund from a payment service provider after having fallen victim of bank employee impersonation fraud and is introducing another refund claim to the same payment service provider after having been again victim of the same type of fraud could be considered as 'gross negligence' as that might indicate a high level of carelessness from the user who should have been more vigilant after having already be victim of the same fraudulent *modus operandi*.

(83) Contractual terms and conditions relating to the provision and use of a payment instrument, the effect of which would be to increase the burden of proof on the consumer or to reduce the burden of proof on the issuer, should be considered null and void. Moreover, in specific situations and in particular where the payment instrument is not present at the point of sale, such as in the case of online payments, it is appropriate to require the payment service provider to provide evidence of alleged negligence since the payer's means to do so are very limited in such cases.

(84) Consumers are particularly vulnerable in cases of card-based payment transactions where the exact transaction amount is not known at the moment when the payer gives permission to execute the payment transaction, for example at automatic fuelling stations, in car rental contracts or when making hotel reservations. The payer's payment service provider should be able to block an amount of funds on the payer's payment account in proportion with the amount of the payment transaction which can reasonably be expected by the payer, and only if the payer has given his or her consent for that precise amount to be blocked. Those funds should be released immediately after receipt of the information on the exact final amount of the payment transaction and at the latest immediately after receipt of the payment order. To ensure a prompt release of the difference between the blocked amount and the exact amount of the payment transaction, the payee should inform the payment service provider immediately after the delivery of the service or goods to the payer.

(85) Legacy non-euro direct debit schemes continue to exist in Member States whose currency is not the euro. Those schemes are proving to be efficient and ensure the same high level of protection to the payer by other safeguards, not always based on an unconditional right to a refund. In that case the payer should be protected by the general rule for a refund when the executed payment transaction exceeds the amount which could reasonably have been expected. In addition, it should be possible 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. Users should be able to rely on the proper execution of a complete and valid payment order if the payment service provider has no contractual or statutory ground for refusal. If the payment service provider refuses a payment order, the refusal and the reason for the refusal should be communicated to the payment service user at the earliest opportunity, subject to the requirements of Union and national law. Where the framework contract provides that the payment service provider may charge a fee for refusal, such a fee should be objectively justified and should be as low as possible.

(87) In view of the speed with which fully automated payment systems process payment transactions, which means that after a certain point in time payment orders cannot be revoked without high manual intervention costs, it is necessary to lay down a clear deadline for payment revocations. However, depending on the type of the payment service 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.

(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. For all other payments, such as payments initiated by or through a payee, including direct debits and card payments, in the absence of an explicit agreement between the payment service provider and the payer setting a longer execution time, the same 1-day execution time should apply. It should be possible to extend those periods by 1 additional business day, if a payment order is given on paper, to allow the continued provision of payment services to consumers who are used only to paper documents. When a direct debit scheme is used the payee's payment service provider should transmit the collection order within the time limits agreed between the payee and the payment service provider, enabling settlement on the agreed due date. It should be possible to maintain or establish rules specifying an execution time shorter than 1 business day.

(91) The rules on execution for the full amount and execution time should constitute good practice where one of the payment service providers is not located in the Union. When making a credit transfer or money 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. The payment service provider of the payer should act with due diligence and verify, where technically possible and without requiring manual intervention, the coherence of the unique

identifier, and, where the unique identifier is found to be incoherent, to refuse the payment order and inform the payer thereof.

(94) The smooth and efficient functioning of payment systems depends on the user being able to rely on the payment service provider executing the payment transaction correctly and within the agreed time. Usually, the payment service provider is able to assess the risks involved in a payment transaction. It is the payment service provider that provides the payments system that makes arrangements to recall misplaced or wrongly allocated funds and decides in most cases on the intermediaries involved in the execution of a payment transaction. In view of all of those considerations, it is appropriate, except under abnormal and unforeseeable circumstances, to impose liability on the payment service provider in respect of the execution of a payment transaction accepted from the user, except in respect of acts and omissions by the payee's payment service provider, who was selected solely by the payee. However, in order not to leave the payer unprotected in the unlikely circumstances that it is not clear that the payment amount was duly received by the payee's payment service provider, the corresponding burden of proof should lie on the payer's payment service provider. As a rule, it can be expected that the intermediary institution, usually an impartial body such as a central bank or a clearing house, that transfers the payment amount from the sending to the receiving payment service provider, will store the account data and will be able to provide the data where necessary. Where the payment amount has been credited to the receiving payment service provider's account, the payee should immediately have a claim against the payment service provider for credit of the account.

(95) The payer's payment service provider, namely the account servicing payment service provider or, where appropriate, the payment initiation service 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.

(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,[50] including the principles of purpose limitation, data minimisation and storage limitation. Data protection by design and data protection by default should be embedded in all data processing systems developed and used within the framework of this Regulation. Therefore, the supervisory authorities under Regulation (EU) 2016/679 and Regulation (EU) 2018/1725 should be responsible for the supervision of processing of personal data carried out in the context of this Regulation.

(98) As acknowledged in the Communication from the Commission on a Retail Payments Strategy for the EU, the good functioning of EU payments markets is of substantial public interest. Therefore, when it is necessary in the context of this Regulation for the provision of payment services and for the compliance with this Regulation, payment service providers and payment system operators should be able to process special categories of personal data as defined in Article 9(1) of Regulation (EU) 2016/679 and Article 10(1) of Regulation (EU) 2018/1725. Where special categories of personal data are processed, payment service providers and payment system operators should implement appropriate technical and organisational measures to safeguard the fundamental rights and freedoms of natural persons. Those measures should include technical limitations on the re-use of data and the use of state-of-the-art security and privacy-preserving measures, including pseudonymisation, or encryption to ensure compliance with the principles of purpose limitation, data minimisation and storage limitation, as laid down in Regulation (EU) 2016/679. The payment service providers and payment systems should also implement specific organisation measures, including training on processing such data, limiting access to special categories of data and recording such access.

(99) The provision of information to individuals about the processing of personal data should be carried out in accordance with Regulation (EU) 2016/679 and Regulation (EU) 2018/1725.

(100) Fraudsters often target the most vulnerable individuals of our society. The timely detection of fraudulent payment transactions is essential, and transaction monitoring plays an import role in that detection. It is therefore appropriate to require payment service providers to have in place transaction monitoring mechanisms, reflecting the crucial contribution of those mechanisms to fraud prevention, going beyond the protection offered by strong customer authentication, in respect of payment transactions, including transactions involving payment initiation services.

(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.

---

[50] 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).

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

(103) Fraud in credit transfers is inherently adaptive and comprises an open-ended diversity of practices and techniques, including the stealing of authentication credentials, invoice tampering, and social manipulation. Therefore, to be able to prevent ever new types of fraud, transaction monitoring should be constantly improved, making full use of technology such as artificial intelligence. Often one payment service provider does not have the full picture about all elements that could lead to timely fraud detection. However, it can be made more effective with a greater amount of information on potentially fraudulent activity stemming from other payment service providers. Therefore, sharing of all relevant information between payment service providers should be possible. To better detect fraudulent payment transactions and protect their customers, payment services providers should, for the purpose of transaction monitoring, make use of payment fraud data shared by other payment services providers on a multilateral basis such as dedicated IT platforms based on information sharing arrangements. To improve the protection of payers against fraud in credit transfers, payment service providers should be able to rely on information as comprehensive and up to date as possible, namely by collectively using information concerning unique identifiers, manipulation techniques and other circumstances associated with fraudulent credit transfers identified individually by each payment services provider. Before concluding an information sharing arrangement, payment service providers should carry out a data protection impact assessment, in accordance with Article 35 of Regulation (EU) 2016/679. Where the data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons, payment service providers should consult the relevant data protection authority in accordance with Article 36 of that Regulation (EU) 2016/679. A new impact assessment should not be required when a payment service provider joins an existing information sharing arrangement for which a data protection impact assessment has already been carried out. The information sharing arrangement should lay down technical and organisational measures to protect personal data. It should lay down roles and responsibilities under data protection laws, including in case of joint controllers, of all payment service providers.

(104) For the purpose of exchanging personal data with other payment service providers who are subject to information sharing arrangements, 'unique identifier' should be understood as referring to 'IBAN' as defined in Article 2 point 15 of Regulation (EU) 260/2012.

(105) To prevent legitimate exchanges of information on potentially fraudulent activity leading to unjustified 'de-risking' or withdrawal of payment account services to

payment services users without explanation or recourse, it is appropriate to have safeguards in place. Payment fraud data shared under a multilateral information sharing arrangement that may entail the disclosure of personal data, including unique identifiers of payees potentially involved in fraud in credit transfers, should only be used by payment services providers for the purpose of enhancing transaction monitoring. Additional safeguards should be put in place by payment services providers, such as contacting the customer if he or she is the payer of a credit transfer which can be assumed to be fraudulent, and further monitoring of an account, where the unique identifier shared as potentially fraudulent designates a customer of that payment service provider. Payment fraud data shared amongst payment services providers in the context of such arrangements should not constitute grounds for withdrawal of banking services without detailed investigation.

(106) Payment fraud becomes increasingly sophisticated, with fraudsters using manipulative and impersonating techniques which are difficult for payment service users to detect without a sufficient level of awareness and information about fraud. Payment service providers can play an important role in reinforcing fraud prevention by regularly taking every necessary initiative to increase their payment service users' understanding and awareness about the risks and trends of payment fraud. In particular, payment service providers should run proper awareness raising programmes and campaigns on fraud trends and risks addressed to customers and employees of payment service providers, with the aim of helping customers realise that they are victim of a fraud attempt. Payment service providers should give to their consumers, through various media, adapted information about fraud, giving them clear messages and warnings, helping them to react properly when exposed to potentially fraudulent situations. The EBA should develop guidelines about the different types of programmes to be developed by payment service providers on payment fraud risks, taking into account the ever-changing nature of fraud-related risks.

(107) Security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce. All payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. In the area of fraud, the major innovation of Directive (EU) 2015/2366 was the introduction of Strong Customer Authentication (SCA). The Commission's evaluation of the implementation of Directive (EU) 2015/2366 concluded that strong customer authentication has already been highly successful in reducing fraud.

(108) SCA should not be circumvented notably by any unjustified reliance on SCA exemptions. Clear definitions of Merchant Initiated Transactions (MITs) and of Mail Orders or Telephone Orders (MOTOs) should be introduced since these notions, which may be relied upon to justify non-application of SCA, are diversely understood and applied and are subject to abusive reliance. Regarding MITs, strong customer authentication should be applied at the set-up of the initial mandate, without the need to apply SCA for subsequent merchant-initiated payment transactions. Regarding MOTOs, only the initiation of payment transactions - not their execution - should be non-digital for a transaction to be considered as a MOTO 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.

(109) As the payment service provider that should apply strong customer authentication is the payment service provider that issues the personalised security credentials, payment transactions that are not initiated by the payer but by the payee only should not be subject to strong customer authentication to the extent that those transactions are initiated without any interaction or involvement of the payer. The regulatory approach to MITs and direct debits, both being transactions initiated by the payee, should be aligned and benefit from the same consumer protection measures, including refunds.

(110) To improve financial inclusion, and in line with Directive (EU) 2019/882 of the European Parliament and of the Council[51] 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 of their material incapability of performing SCA. Therefore, payment service providers should ensure that their customers can benefit from various methods to perform SCA which are adapted to their needs and situations. These methods should not depend on one single technology, device or mechanism, or on the possession of a smartphone.

(111) European Digital Identity Wallets implemented under Regulation (EU) No 910/2014[52] of the European Parliament and of the Council, as amended by Regulation [XXX], are electronic identification means that offer identification and authentication tools for accessing financial services across borders, including payment services. The introduction of the European Digital Identity Wallet would further facilitate cross-border digital identification and authentication for secure digital payments and facilitate the development of a pan-European digital payments landscape.

(112) Growth of electronic commerce and mobile payments should be accompanied by a generalised enhancement of security measures. In case of remote initiation of a payment transaction, i.e., when a payment order is placed via the internet, the authentication of transactions should rely on 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

---

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

[52] 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).

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 transaction risk analysis, introducing clear audit requirements, providing more detail and better definitions on risk monitoring requirements and data to share, and to assess the potential benefits of allowing payment service providers to report fraudulent transactions for which they are solely liable. The EBA should develop draft Regulatory Technical Standards laying down rules on transaction risk analysis.

(116) Security measures should be compatible with the level of risk involved in payment services. To allow the development of user-friendly and accessible means of payment for low-risk payments, such as low value contactless payments at the point of sale, whether or not these payments are based on mobile phone, the exemptions to the application of security requirements should be specified in regulatory technical standards. Safe use of personalised security credentials is needed to limit the risks relating to spoofing, phishing and other fraudulent activities. The user should be able to rely on the adoption of measures that protect the confidentiality and integrity of personalised security credentials.

(117) Payment service providers should apply SCA when, *inter alia*, the payment service user is carrying out any action through a remote channel which may imply the risk of payment fraud or other abuses. Payment service providers should have in place adequate security measures to protect the confidentially and integrity of the 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 strong customer authentication within the remit of their role in the initiation or execution of payment transactions. Given the role that they play in ensuring that key security requirements concerning retail payments are properly implemented, including by providing appropriate IT solutions, technical service providers and operators of payment schemes should be held liable for the financial damages caused to payees or to the payment service providers of the payees or of the payers in case they fail to support the application of strong customer authentication.

(121) Member States should designate the competent authorities for granting authorisation to payment institutions and for accreditation and monitoring of alternative dispute resolution (ADR) procedures.

(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[53] 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[54], to resolve disputes before resorting to a court. Designated competent authorities should notify the Commission of a competent quality ADR entity or entities on their territory to resolve national and cross-border disputes and to cooperate with regard to disputes concerning rights and obligations pursuant to this Regulation.

(123) Consumers should be entitled to enforce their rights in relation to the obligations imposed on payment and electronic money service providers under this Regulation through representative actions in accordance with Directive (EU) 2020/1828 of the European Parliament and of the Council'[55].

(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

---

53 OJ L 177, 4.7.2008, p. 6–16.

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

55 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).

the European Parliament and of the Council[56] 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.

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

(126) Member States should be required to provide for effective, proportionate and 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, data protection, competition, consumer protection, audit, police and other enforcement authorities. Member States should ensure that their legal framework allows and facilitates such cooperation as required, to achieve the

[56] 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).

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 is to compel natural or legal persons who are identified as responsible for an ongoing infringement or are required to comply with an order from the investigating competent authority, to comply with that order or terminate the ongoing breach, the application of periodic penalty payments should not prevent competent authorities from imposing subsequent administrative sanctions for the same infringement.

(134) Unless otherwise provided for by Member States, periodic penalty payments should be calculated on a daily basis.

(135) Competent authorities should be empowered by Member States to impose such administrative sanctions and administrative measures on payment services providers or other natural or legal persons where relevant to remedy the situation in the case of infringement. The range of sanctions and measures should be sufficiently broad to allow Member States and competent authorities to take account of the differences between payment service providers, in particular between credit institutions and other payment institutions, as regards their size, characteristics and the nature of the business.

(136) The publication of an administrative sanction or measure for infringement of provisions of this Regulation can have a strong dissuasive effect against repetition of such infringement. Publication also informs other entities of the risks associated with the sanctioned payment services provider before entering into a business relationship and assists competent authorities in other Member States in relation to the risks associated with a payment services provider when it operates in their Member States

on a cross-border basis. For those reasons, the publication of decisions on administrative sanctions and administrative measures should be allowed as long as it concerns legal 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 to update, to take account of inflation, the amounts up to which a payer may be obliged to bear the losses relating to any unauthorised payment transactions resulting from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument. The Commission, when preparing delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.

(139) In order to ensure consistent application of this Regulation, the Commission should be able to rely on the expertise and support of the EBA, which should have the task of preparing guidelines and draft Regulatory and Implementing Technical Standards. The Commission should be empowered to adopt those draft Regulatory Technical Standards. The EBA should, when developing guidelines, draft Regulatory Technical Standards and draft Implementing Technical Standards pursuant to this Regulation and in accordance with Regulation (EU) No 1093/2010, consult all relevant stakeholders, including those in the payment services market, reflecting all interests involved.

(140) The EBA should, in line with Article 9(5) of Regulation (EU) No 1093/2010, be granted product intervention powers to be able to temporarily prohibit or restrict in the Union certain type or a specific feature of a payment service or an electronic money service which is identified as potentially causing harm to consumers, threatening the orderly functioning and integrity of financial markets. Regulation (EU) No 1093/2010 should therefore be amended accordingly.

(141) The Annex to Regulation (EU) 2017/2394 of the European Parliament and of the Council[57] should be amended to include a reference to this Regulation to facilitate cross-border cooperation on the enforcement of this Regulation.

(142) Since the objective of this Regulation, namely further integration of an internal market in payment services, cannot be sufficiently achieved by the Member States because it requires harmonisation of various different rules in Union and national law, but can rather, by reason of its scale and effects, be better achieved at Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.

(143) Considering that this Regulation and Directive (EU) XXX (PSD3) lay down the legal framework governing the provision of retail payment services and electronic money services within the Union, to ensure legal certainty and consistency of the Union's legal framework, this Regulation should apply from the same date as the date of application of the laws, regulations and administrative provisions that Member States are required to adopt to comply with Directive (EU) XXX (PSD3). However, the provisions requiring payment service providers to verify discrepancies between the name and unique identifier of a payee in case of credit transfers and the respective liability regime should apply from 24 months after the date of entry into force of this Regulation, thus granting payment service providers enough time to take the necessary steps to adjust their internal systems, to comply with such requirements.

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

(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

---

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

58 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).

punished twice in criminal proceedings for the same offence. This Regulation must be applied in accordance with those rights and principles.

(146) References to amounts in euro, are to be understood as the national currency equivalent as determined by each non-euro Member State.

(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[59] and delivered an opinion on [XX XX 2023][60],

HAVE ADOPTED THIS REGULATION:

TITLE I

SUBJECT MATTER, SCOPE AND DEFINITIONS

Article 1

Subject matter

1. This Regulation lays down uniform requirements on the provision of payment services and electronic money services, as regards:
   (a) the transparency of conditions and information requirements for payment services and electronic money services;
   (b) the respective rights and obligations of payment and electronic money service users, and of payment and electronic money service providers in relation to the provision of payment services and electronic money services.
2. Unless specified otherwise, any reference to payment services shall be understood in this Regulation as meaning payment and electronic money services.
3. Unless specified otherwise, any reference to payment service providers shall be understood in this Regulation as meaning payment service providers and electronic money service providers.

Article 2

Scope

1. This Regulation applies to payment services provided within the Union by the following categories of payment service providers:

[59] 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).

[60] OJ C […], […], p. […].

(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[61], 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.

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

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

(b) payment transactions from the payer to the payee through a commercial agent, as defined in Article 1(2) of Directive 86/653/EEC, provided that all of following conditions are met : i) the commercial agent is authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee, but not both of them, irrespective of whether or not the commercial agent is in the possession of the client's funds, and ii) such agreement gives the payer or the payee a real margin to negotiate with the commercial agent or conclude the sale or purchase of goods or services;

(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 cash is provided in retail stores following an explicit request by the payment service user but independently of the execution of any payment transaction and without any obligation to make a purchase of goods and services. The payment service user shall be provided with information on any possible charges for this service before the requested cash is provided;

(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;

[61] 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).

(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;

(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;

(i) without prejudice to Article 23(2), and Articles 58 and 87, services provided by technical service providers;

(j) services based on specific payment instruments that meet one of the following conditions:

(i) instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a single limited network of service providers under direct commercial agreement with a professional issuer;

(ii) instruments which can be used only to acquire a very limited range of goods or services;

(iii) instruments valid only in a single Member State, which are provided at the request of an undertaking or a public sector entity and regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer;

(k) payment transactions by a provider of electronic communications networks as defined in Article 2, point (1), of Directive (EU) 2018/1972 of the European Parliament and of the Council[62], or services provided in addition to electronic

[62] 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).

communications services as defined in Article 2, point (4), of that Directive to a subscriber to the network or service:

(i) to purchase digital content and voice-based services, regardless of the device used for the purchase or consumption of the digital content and charged to the related bill; or

(ii) performed from or via an electronic device and charged to the related bill within the framework of a charitable activity or for the purchase of tickets;

provided that the value of any single payment transaction does not exceed EUR 50 and:

– the cumulative value of payment transactions for an individual subscriber does not exceed EUR 300 per month, or

– where a subscriber pre-funds its account with the provider of the electronic communications network or service, the cumulative value of payment transactions does not exceed EUR 300 per month;

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

(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.

3. Titles II and III apply to payment transactions in the currency of a Member State where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union.

4. Title II, except for Article 13(1), point (b) , Article 20, point (2)(e) and Article 24, point (a), and Title III, except for Articles 67 to 72, apply to payment transactions in a currency that is not the currency of a Member State, where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.

5. Title II, except for Article 13(1), point (b), Article 20, point (2)(e) and point (5)(h) and Article 24, point (a), and Title III, except for Article 28(2) and (3), Articles 62, 63 and 67, Article 69(1), and Articles 75 and 78, apply to payment transactions in all currencies where only one of the payment service providers is located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.

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 either of the following:

(a) the Member State in which the payment service provider has its registered office; or

(b) if the payment service provider has, under its national law, no registered office, the Member State in which the payment service provider has its head office;

(2) 'host Member State' means the Member State other than the home Member State in which a payment service provider has an agent, a distributor or a branch or provides payment services;

(3) 'payment service' means any business activity set out in Annex I;

(4) 'payment institution' means a legal person that has been granted authorisation in accordance with Article 13 of Directive (EU) [PSD3] to provide payment services or electronic money services throughout the Union;

(5) 'payment transaction' means an act of placing, transferring or withdrawing funds, based on a payment order placed by the payer, or on his behalf, or by the payee, or on his behalf, irrespective of any underlying obligations between the payer and the payee;

(6) 'initiation of a payment transaction' means the steps necessary to prepare the execution of a payment transaction, including the placement of a payment order and the completion of the authentication process;

(7) 'remote initiation of a payment transaction' means a payment transaction for which a payment order is placed via the internet;

(8) 'execution of a payment transaction' means the process starting once the initiation of a payment transaction is completed and ending once the funds placed, withdrawn, or transferred are available to the payee;

(9) ‘payment system’ means a funds transfer system with formal and standardised arrangements and common rules for the processing, clearing or settlement of payment transactions;

(10) ‘payment system operator’ means the legal entity legally responsible for operating a payment system;

(11) ‘payer’ means a natural or legal person who holds a payment account and places a payment order from that payment account, or, where there is no payment account, a person who places a payment order;

(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 is 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 payer;

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

(21) ‘account information service’ means an online service of collecting, either directly or through a technical service provider, and consolidating information held on one or more payment accounts of a payment service user with one or several account servicing payment service providers;

(22) ‘payment initiation service provider’ means a payment service provider providing payment initiation services;

(23) ‘account information service provider’ means a payment service provider providing account information services;

(24) ‘consumer’ means a natural person who, in payment service contracts covered by this Regulation, is acting for purposes other than his or her trade, business or profession;

(25) ‘framework contract’ means a payment service contract which governs the future execution of individual and successive payment transactions and which may contain the obligation and conditions for setting up a payment account;

(26) ‘money remittance’ means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, or where such funds are received on behalf of and made available to the payee;

(27) ‘direct debit’ means a payment service for debiting a payer’s payment account, where a payment transaction is initiated by the payee on the basis of a mandate given by the payer to the payee, to the payee’s payment service provider or to the payer’s own payment service provider;

(28) ‘credit transfer’ means a payment service, including instant credit transfers, for crediting a payee’s payment account with a payment transaction or a series of payment transactions from a payer’s payment account by the payment service provider which holds the payer’s payment account, based on an instruction given by the payer;

(29) ‘instant credit transfer’ means a credit transfer which is immediately executed, regardless of the day or hour;

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

(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 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;

(44) ‘agent’ means a natural or legal person who acts on behalf of a payment institution in providing payment services, with the exclusion of electronic money services;

(45) ‘branch’ means a place of business other than the head office which is a part of a payment institution, which has no legal personality and which carries out directly some or all of the transactions inherent in the business of a payment institution; all of the places of business set up in the same Member State by a payment institution with a head office in another Member State shall be regarded as a single branch;

(46) ‘group’ means a group of undertakings that are linked to each other by a relationship as referred to in Article 22(1), points (2) or (7) of Directive 2013/34/EU of the European Parliament and of the Council[63] or undertakings as referred to in Articles 4, 5, 6 and 7 of Commission Delegated Regulation (EU) No 241/2014[64], which are linked to each other by a relationship as referred to in Article 10(1) or Article 113(6), first subparagraph, or 113(7), first subparagraph of Regulation (EU) No 575/2013;

(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;

---

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

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

(50) ‘electronic money’ means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on the receipt of funds for the purpose of making payment transactions and which is accepted by other natural or legal persons than the issuer;

(51) ‘distributor’ means a natural or legal person that distributes or redeems electronic money on behalf of a payment institution;

(52) ‘electronic money services’ means the issuance of electronic money, the maintenance of payment accounts storing electronic money units, and the transfer of electronic money units;

(53) ‘commercial trade name’ means the name which is commonly used by the payee to identify itself to the payer;

(54) ‘ATM deployer’ means operators of automated teller machines who do not service payment accounts.

(55) ‘payment institution providing electronic money services’ means a payment institution which provides the services of issuance of electronic money, maintenance of payment accounts storing electronic money units, and transfer of electronic money units, whether or not it also provides any of the services referred to in Annex I.

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. Payments 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.

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.

2. Where, for the use of a given payment instrument, the payment service provider or another party involved in the transaction requests a charge, it shall inform the payment service user thereof prior to the initiation of the payment transaction.

3. The payer shall only be obliged to pay for the charges referred to in paragraphs 1 and 2 if their full amount was made known prior to the initiation of the payment transaction.

Article 7

Information requirements applicable to cash withdrawal services

Natural or legal persons providing cash withdrawal services as referred to in Article 38 of Directive (EU) [PSD3] shall provide or make available to their customers information on any charges before the customer carries out the withdrawal as well as upon receipt of the cash 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

In cases of payment instruments which, according to the relevant framework contract, concern only individual payment transactions that do not exceed EUR 50 or that either have a spending limit of EUR 200 or store funds that do not exceed EUR 200 at any time:

(a) by way of derogation from Articles 19, 20 and 24, the payment service provider shall provide the payer only with information on the main characteristics of the payment service, including the way in which the payment instrument can be used, liability, charges levied and other material information needed for the payer to take an informed decision as well as an indication of where any other information and conditions specified in Article 20 are made available in an easily accessible manner;

(b) it may be agreed by the parties to the framework contract that, by way of 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.

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

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) the estimated time for the funds of credit transfers and money remittance transactions to be received by the payment service provider of the payee located outside the Union;

(d) all charges payable by the payment service user to the payment service provider and, where applicable, a breakdown of those charges;

(e) where applicable, the actual or reference exchange rate to be applied to the payment transaction;

(f) where applicable, the estimated charges for currency conversion in relation to credit transfers and money remittance transactions, expressed as a percentage mark-up over the latest available applicable foreign exchange reference rate issued by the relevant central bank;

(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;

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

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, distributor or branch established in the Member State where the payment service is offered, and any other address, including electronic mail address, relevant for communication with the payment service provider;

(ii) the particulars of the relevant supervisory authorities designated under Directive (EU) [PSD3] and of the register provided for in Articles 17 and 18 of that Directive or of any other relevant public register of authorisation of the payment service provider and the registration number or equivalent means of identification in that register;

(b) on the use of the payment service:

(i) a description of the main characteristics of the payment service to be provided;

(ii) a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly placed or executed;

(iii) the form of and procedure for placing a payment order or giving permission to execute a payment transaction and withdrawal of such permission in accordance with Articles 49 and 66;

(iv) a reference to the time of receipt of a payment order in accordance with Article 64 and the cut-off time, if any, established by the payment service provider;

(v) the maximum execution time for the payment services to be provided;

(vi) the estimated time for the funds of credit transfers to be received by the payment service provider of the payee located outside the Union;

(vii) whether there is a possibility to agree on spending limits for the use of the payment instrument in accordance with Article 51(1);

(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 provider not servicing payment accounts when offering cash withdrawal services;

(iii) where applicable, the interest and exchange rates to be applied or, if reference interest and exchange rates are to be used, the method of

calculating the actual interest, and the relevant date and index or base for determining such reference interest or exchange rate;

(iv) where agreed, the immediate application of changes in reference interest or exchange rate and information requirements relating to the changes in accordance with Article 22(3);

(v) where applicable, the estimated charges for currency conversion services in relation to a credit transfer expressed as a percentage mark-up over the latest available applicable foreign exchange reference rate issued by the relevant central bank;

(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) where agreed, the conditions under which the payment service provider reserves the right to block a payment instrument in accordance with Article 51;

(iv) the liability of the payer in accordance with Article 57(5), Article 59(3) and Article 60, including information on the relevant amount;

(v) how and within what period of time the payment service user is to notify the payment service provider, and the police in case of impersonation fraud referred to in Article 59, of any unauthorised or incorrectly initiated or executed payment transaction or of any authorised credit transfer made following an incorrect application of the name and unique identifier matching verification service or impersonation fraud, in accordance with Article 54;

(vi) the payment service provider's liability for unauthorised payment transactions in accordance with Article 56, for the incorrect application of the name and unique identifier matching verification service in

accordance with Article 57, and for impersonation fraud in accordance with Article 59;

(vii) the liability of the payment service provider for the initiation or execution of payment transactions in accordance with Articles 75 and 76;

(viii) the conditions for refund in accordance with Articles 62 and 63;

(f) on changes to, and termination of, the framework contract:

(i) where agreed, information that the payment service user will be deemed to have accepted changes in the conditions in 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 in conditions of the framework contract

1. The payment service provider shall propose any changes in the framework contract or in the information and conditions set out in Article 20 in the same way as provided for in Article 19(1) and no later than 2 months before their proposed date of application. The payment service user can either accept or reject the changes before the date of their proposed date of entry into force.

2. Where applicable, in accordance with Article 20, point (f)(i), the payment service provider shall inform the payment service user that the payment service user is to be deemed to have accepted those changes if the 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 6 months. Charges, if any, for termination of the framework contract shall be appropriate and in line with costs. Where, under the framework contract, payment services are offered jointly with technical services aimed at supporting the provision of payment services and provided by the payment service provider or by a third party the payment service provider has partnered with, such technical services shall be subject to the same framework contract requirements on termination fees.

3. If agreed in the framework contract, the payment service provider may terminate a framework contract concluded for an indefinite period by giving at least 2 months' notice in the same way as provided for in Article 19(1).

4. Charges for payment services levied on a regular basis shall be payable by the payment service user only proportionally up to the termination of the contract. If such charges are paid in advance, those charges shall be reimbursed proportionally by the payment service provider.

5. The provisions of this Article are without prejudice to the Member States' laws and regulations governing the rights of the parties to declare the framework contract unenforceable or void.

6. Member States may provide for more favourable provisions on termination for payment service users.

7. Member States shall by [OP please insert the date = data of application of this Regulation] notify to the Commission the provisions of their law adopted pursuant to paragraph 6. They shall, without delay, notify any subsequent amendment to such provisions.

Article 24

Information before execution of individual payment transactions

In the case of an individual payment transaction initiated by the payer under a framework contract, a payment service provider shall, at the payer's request for this specific payment transaction, provide explicit information on all of the following:

(a) the maximum execution time;

(b) the charges payable by the payer;

(c) where applicable, a breakdown of the amounts of any charges.

Article 25

Information for the payer on individual payment transactions

1. After the amount of an individual payment transaction is debited from the 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;

   (b) the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency used for the payment order;

   (c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges, or the interest payable by the payer;

   (d) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider, and the amount of the payment transaction after that currency conversion;

   (e) the debit value date or the date of receipt of the payment order.

2. A framework contract shall include a condition that the payer may require the information referred to in paragraph 1 to be provided or made available periodically, at least once a month, free of charge and in an agreed manner which allows the payer to store and reproduce information unchanged.

3. Member States may require payment service providers to provide information on paper or on another durable medium at least once a month, free of charge.

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 of EUR 200, or store funds which do not exceed EUR 200 at any time, payment service providers may agree with their payment service users that:

   (a) Article 52, point (b), Article 53(1), points (c) and (d) , and Article 60(4) do not apply if the payment instrument does not allow its blocking or prevention of its further use;

   (b) Articles 55 and 56, and Article 60(1) and (4), do not apply if the payment instrument is used anonymously or the payment service provider is not in a position for other reasons which are intrinsic to the payment instrument to prove that a payment transaction was authorised;

   (c) by way of derogation from Article 65(1), the payment service provider is not required to notify the payment service user of the refusal of a payment order, if the non-execution is apparent from the context;

   (d) by way of derogation from Article 66, the payer shall not revoke the payment order after transmitting the payment order or authorising the payment transaction to the payee;

   (e) by way of derogation from Articles 69 and 70, other execution periods apply.

2. Articles 56 and 60 shall apply also to electronic money, except where the payer's 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 providing electronic money services shall not grant to the holder of electronic money interest or any other benefit related to the length of time during which he or she holds the electronic money.

CHAPTER 2

Access to payment systems and to accounts maintained with credit institutions

Article 31

Access to payment systems

1. Payment system operators shall have in place objective non-discriminatory, transparent and proportionate rules on access to a payment system by authorised or registered payment service providers that are legal persons. Payment system operators shall not inhibit access to a payment system more than is necessary to safeguard against specific risks, including where applicable settlement risk, operational risk, credit risk, liquidity risk and business risk or more than is necessary to protect the financial and operational stability of the payment system.

2. A payment system operator shall make publicly available its rules and procedures for admission to participation to that payment system and the criteria and methodology it uses for risk assessment of applicants for participation.

3. Upon receiving an application for participation by a payment service provider, a payment system operator shall assess the relevant risks of granting the applicant payment service provider access to the system. A payment system operator shall only refuse participation to an applicant payment service provider where the applicant poses risks to the system, as referred to in paragraph 1. The payment system operator shall notify that applicant payment service provider in writing whether the request for participation is granted or refused and shall provide full reasons for any refusal.

4. Paragraphs 1, 2 and 3 shall not apply to payment systems composed exclusively of payment service providers belonging to the same group.

5. Payment system operators shall not have in place any of the following requirements:

(a) restrictive rules on effective membership in other payment systems;

(b) rules which discriminate between authorised payment service providers or between registered payment service providers in relation to the rights, obligations and entitlements of members;

(c) restrictions on the basis of institutional status.

6. A participant of a payment system that allows an authorised or registered payment service provider that is not a participant of the payment system to pass transfer orders through that payment system shall, when requested, give the same possibility to other authorised or registered payment service providers in an objective, proportionate, transparent and non-discriminatory manner. In case of a rejection of such request, the participant of a payment system shall provide any requesting payment service provider with full reasons for such rejection.

7. For payment systems that are not covered by Eurosystem oversight, pursuant to Regulation (EU) No 795/2014, Member States shall designate a competent authority responsible for oversight of payment systems to ensure enforcement of paragraphs 1 2, 3, 5 and 6 by payment systems governed by their national law.

Article 32

Provision by credit institutions of payment accounts to payment institutions

1. A credit institution shall only refuse to open or shall only close a payment account for a payment institution for its agents or distributors or for an applicant for a license as a payment institution in the following cases:

(a) The credit institution has serious grounds to suspect defective money laundering or terrorism financing controls by the applicant or that illegal activities are being committed either by the applicant or its customers;

(b) there is or has been a breach of contract committed by the applicant for an account;

(c) insufficient information and documents have been received from the applicant for an account;

(d) the applicant for an account or its business model presents an excessive risk profile;

(e) the applicant for an account would present a disproportionately high compliance cost for the credit institution.

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

3. A credit institution shall notify to the payment institution or to its agents or distributors, or to the applicant for a license as a payment institution, any decision to refuse to open or to close a payment account to a payment institution or to its agents or distributors, or to an applicant for a license as a payment institution; it shall duly motivate any such decision. Such motivation must be specific to the risks posed by the activity or planned activity of that payment institution or of its agents or distributors, as assessed by the credit institution, and not be generic in nature.

4. A payment institution or its agents or distributors, or an applicant for a license as a payment institution which is the subject of a 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. 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. 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. Without prejudice to Articles 38 and 39, account servicing payment service providers that offer to a payer a payment account that is accessible online and have put in place a dedicated interface as referred to in paragraph 1 of this Article, shall not be obliged to also maintain permanently another interface as fall-back for the purpose of data exchange with account information and payment initiation service providers.

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

without delay, upon request by authorised payment initiation service providers, account information service providers or by payment service providers that have applied to their competent authorities for the relevant authorisation and shall make a summary of that documentation publicly available on their website.

4. Account servicing payment service providers shall ensure that, except for emergency situations which prevent them from doing so, any change to the technical specifications of their dedicated interface referred to in paragraph 1 is made available to authorised payment initiation service providers, account information service providers, or payment service providers that have applied to their competent authorities for the relevant authorisation, in advance, as soon as possible and not less than 3 months before the change is implemented. Account servicing payment service providers shall document emergency situations where changes were implemented without such advance information and make the documentation available to competent authorities on request.

5. Account servicing payment service providers shall publish on their website quarterly statistics on the availability and performance of their dedicated interface. The performance of the dedicated interfaces shall be measured by the number of successful account information requests over the total number of account information requests, and by the number and transaction volume of the successful payment initiation requests over the total number and transaction volume of the total number of payment initiation requests.

6. Account servicing payment service providers shall make available a testing facility, including support, for connection to the dedicated interfaces and functional testing to enable authorised payment initiation service providers and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users. No sensitive payment data or any other personal data shall be shared through the testing facility.

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 permission of the payment service user given to the account information service provider or the payment initiation service providers in accordance with Article 49(2);

(c) make use, in a non-discriminatory manner, of any authentication exemptions applied by the account servicing payment service provider;

(d) see, prior to initiation of the payment in the case of payment initiation service providers, the unique identifier of the account, the associated names of the account holder and the currencies as available to the payment service user.

3. Account servicing payment service providers shall allow account information service providers to communicate securely, via the dedicated interface, to request and receive information on one or more designated payment accounts and associated payment transactions.

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 or a direct debit;

(b) initiate a single payment;

(c) initiate and revoke a future dated payment;

(d) initiate payments to multiple beneficiaries;

(e) initiate payments, regardless of whether the payee is on the payer's beneficiaries list;

(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;

(h) initiate a payment with one single strong customer authentication, provided the payment initiation service provider has provided the account servicing payment service provider with all of the following:

(i) the payer's unique identifier,

(ii) the payee's legal and commercial name and 'unique identifier',

(iii) a transaction reference,

(iv) the payment amount and the currency of the payment, based on which the single strong customer authentication is triggered.

5. Account servicing payment service providers shall ensure that the dedicated interface provides to payment initiation service providers:

(a) the immediate confirmation, upon request, in a simple 'yes' or 'no' format, of whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer;

(b) the confirmation from the account servicing payment service provider that the payment will be executed on the basis of the information available to the account servicing payment service provider, taking into account any pre-existing payment orders that might affect the full execution of the payment order being placed.

The information referred to in point (b) shall not be shared with the payment initiation service provider but may be used by the account servicing payment service provider in order to provide confirmation of the execution of the operation.

Article 37

Data access parity between dedicated access interface and customer interface

1. Without prejudice to Article 36, account servicing payment service providers shall ensure that their dedicated interface referred to in Article 35(1) offers at all times at least the same level of availability and performance, including technical and IT support, as the interfaces that account servicing payment service providers make available to the payment service user for directly accessing its payment account online.

2. Account servicing payment service providers shall provide account information services providers with at least the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data.

3. Account servicing payment service providers shall provide payment initiation service providers with at least the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the payment service user. That information shall be provided immediately after receipt of the payment order and on an ongoing basis until the payment is final.

Article 38

Contingency measures for an unavailable dedicated interface

1. Account servicing payment service providers shall take all measures in their power to prevent unavailability of the dedicated interface. Unavailability shall be presumed to have arisen when five consecutive requests for access to information for the

provision of payment initiation services or account information services receive no response from the account servicing payment service provider's dedicated interface within 30 seconds.

2. In case of unavailability of the dedicated interface, account servicing payment service providers shall inform payment service providers making use of the dedicated interface of measures taken to restore the interface and of the time estimated necessary for the problem to be resolved. During the period of unavailability, account servicing payment service providers shall offer to account information and payment initiation service providers without delay an effective alternative solution, such as the use of the interface that the account servicing payment service provider uses for authentication and communication with its users, to access payment account data.

3. Where the dedicated interface is unavailable and the account servicing payment service provider has not offered a rapid and effective alternative solution referred to in paragraph 2, payment initiation service providers or account information service providers may request their competent authority, providing all necessary information and evidence, to allow them to use the interface that the account servicing payment service provider uses for authentication and communication with its users for payment account data access.

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

5. The competent authority shall take a decision without undue delay on any request introduced under paragraph 3. As long as the competent authority has not taken a decision on the request, the requesting payment initiation service provider or account information service provider may exceptionally access payment accounts data via an interface that the account servicing payment service provider uses for authentication and communication with its users. The requesting payment initiation service provider or account information service provider shall cease to do so when the dedicated interface is restored to availability, or when the competent authority adopts a decision not authorising such use, whichever is the sooner.

6. In cases where account servicing payment service providers are obliged to allow account information service providers or payment initiation service providers to access the interface that account servicing payment service providers use for authentication and communication with their users, account servicing payment service providers shall immediately make available any technical specifications needed by account information service providers or payment initiation service providers to adequately connect to the interface that the account servicing payment service provider uses for authentication and communication with its users.

7. When accessing the interface that the account servicing payment service provider uses for authentication and communication with its users, the account information

service providers or payment initiation service providers shall meet all requirements laid down in Article 45(2). In particular, the account information service providers or payment initiation service providers shall always duly identify themselves with the account servicing payment services provider.

Article 39

Derogation from having a dedicated interface for data access

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

2. The EBA shall develop draft regulatory technical standards which shall specify the criteria on the basis of which, in accordance with paragraph 1, an account servicing payment service provider may be exempted from the obligation to have in place a dedicated interface and be allowed either to provide, as interface for secure data exchange with account information service providers and payment initiation service providers, the interface that it makes available to its payment user for accessing its payment accounts online or, where appropriate, not to have any interface at all for secure data exchange.

   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 from a payment initiation service provider, provide or make available all information on the initiation of the payment transaction and all information accessible to the account servicing

payment service provider regarding the execution of the payment transaction to the payment initiation service provider;

(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 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.

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 permissions the payment service user has given for the purpose of account information services or payment initiation services covering multiple or recurrent payments.

2. The dashboard shall:

   (a) provide the payment service user with an overview of each ongoing permission given for the purposes of account information services or payment initiation services, including:

      (i) the name of the account information service provider or payment initiation service provider to which access has been granted;

      (ii) the customer account to which access has been granted;

      (iii) the purpose of the permission;

      (iv) the period of validity of the permission;

      (v) the categories of data being shared.

   (b) allow the payment service user to withdraw data access for a given account information service or payment initiation service provider;

   (c) allow the payment service user to re-establish any data access withdrawn;

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

3. The account servicing payment service provider shall ensure that the dashboard is easy to find in its user interface and that information displayed on the dashboard is clear, accurate and easily understandable for the payment service user.

4. The account servicing payment service provider and the account information service or payment initiation service provider to which permission has been granted shall cooperate to make information available to the payment service user via the dashboard in real-time. For the purposes of paragraph 2 points (a), (b), (c) and (e):

   (a) The account servicing payment service provider shall inform the account information service or payment initiation service provider in real time of changes made to a permission concerning that provider made by a payment service user via the dashboard;

   (b) An account information service or payment initiation service provider shall inform the account servicing payment service provider in real time of a new

permission granted by a payment service user regarding a payment account provided by that account servicing payment service provider, including:

(i) the purpose of the permission granted by the payment service user;

(ii) the period of validity of the permission;

(iii) the categories of data concerned.

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 the following:

(a) preventing the use by payment initiation services providers or account information services providers of the credentials issued by account servicing payment service providers to their payment services users;

(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 additional checks of the permission given by the payment service users to a payment initiation service provider or an account information services provider;

(d) requiring additional registrations by payment initiation and account information services providers to be able to access the payment services user's payment account or the dedicated interface;

(e) requiring, unless indispensable to facilitate the exchange of information between account servicing payment service providers and payment initiation and account information services providers related, in particular, to the updating of the dashboard referred to in Article 43, that payment initiation and account information services providers pre-register their contact details 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;

(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 this is the sole method of carrying out the authentication of the payment services user that is supported by an account servicing payment service provider;

(l) requiring two strong customer authentications in a payment initiation service-only journey where the payment initiation service provider transmits to the account servicing payment service provider all the information necessary to initiate the payment, namely one strong customer authentication for the yes/no confirmation and a second strong customer authentication for payment initiation.

2. For the activities of payment initiation services and account information services the name and the account number of the account owner shall not constitute sensitive payment data.

SECTION 4

RIGHTS AND OBLIGATIONS OF ACCOUNT INFORMATION SERVICE PROVIDERS AND PAYMENT INITIATION SERVICE PROVIDERS

Article 45

Use of the customer interface by account information service providers and payment initiation service providers

1. Account information service providers and payment initiation service providers shall access payment account data exclusively via the dedicated interface referred to in Article 35, except in the circumstances covered by Article 38(4) and (5) and Article 39.

2. Where an account information service provider or a payment initiation service provider accesses payment account data via an interface that the account servicing payment service provider makes available to its payment service users for directly accessing their payment account, in accordance with Article 38(4) and (5), or where that is the only interface accessible in accordance with Article 39, the account information service provider or the payment initiation service provider shall at all times:

(a) identify itself towards the account servicing payment service provider;

(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) log the data that are accessed through the interface operated by the account servicing payment service provider for its payment service users, and provide, upon request and without undue delay, the log files to the competent authority. Logs shall be deleted 3 years after their creation. Logs may be kept for longer than this retention period if they are required for monitoring procedures that are already underway.

For the purpose of point (d) logs shall be deleted 3 years after their creation. Logs may be kept for longer than this retention period if they are required for monitoring procedures that are already underway.

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 permission, in accordance with Article 49;

(c) not hold at any time the payer's funds in connection with the provision of the payment initiation service;

(d) ensure that the personalised security credentials of the payment services user are not, with the exception of the payer and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

(e) ensure that any other information about the payment services user obtained when providing payment initiation services, is only provided to the payee and only with the payment services user's permission;

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

2. Payment initiation service providers shall not:

(a) store sensitive payment data of the payment service user;

(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 permission, in accordance with Article 49;

   (b) ensure that the personalised security credentials of the payment service user are not accessible to other parties, with the exception of the user and the issuer of the personalised security credentials, and that when those credentials are transmitted by the account information service provider, transmission is done through safe and efficient channels;

   (c) for each communication session, identify itself towards the account servicing payment service provider of the payment service user and securely communicate with the account servicing payment service provider and the payment service user;

   (d) access only information from designated payment accounts and associated payment transactions;

   (e) have in place suitable and effective mechanisms that prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the payment service user's permission.

2. The account information service provider shall not:

   (a) request sensitive payment data linked to the payment accounts;

   (b) use, access or store any data for purposes other than for performing the account information service permitted by the payment service user, in accordance with Regulation (EU) 2016/679.

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 Article 35(1) and that any identified prohibited obstacle listed in Article 44 is immediately removed by the relevant account servicing payment service provider. Where such non-compliance of the dedicated interfaces with this

Regulation or obstacles are identified, including on the basis of information transmitted by payment initiation services and account information services providers, the competent authorities shall take without delay the necessary enforcement measures and impose any appropriate sanction or, where appropriate, grant access rights in accordance with Article 38(4).

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 regular joint meetings with account servicing payment service providers, payment initiation service and account information service providers and shall deploy their best efforts to ensure that possible issues arising from the use of and access to data exchange interfaces between account servicing payment service providers, payment initiation service and account information service providers are rapidly et durably solved.

7. Account servicing payment service providers shall provide competent authorities with data on access by account information service providers and payment initiation service providers to payment accounts which they service. Competent authorities may also, where appropriate, require account information service providers and payment initiation service providers to provide any relevant data on their operations. In accordance with its powers pursuant to Article 29, point (b), Article 31 and Article 35(2) of Regulation (EU) No 1093/2010, the EBA shall coordinate that monitoring activity by competent authorities, avoiding data reporting duplication. The EBA shall report every two years to the Commission on 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 permission 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.

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 permission 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 permission, 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 permission given by the payment service user to the account information service provider or payment initiation service provider.

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

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

7. The payment service user may withdraw permission to execute a payment transaction or to access a payment account for the purpose of payment initiation services or account information services may be withdrawn by the payment service user at any time. The payment service user may also withdraw permission to execute a series of payment transactions, in which case any future payment transaction shall be considered to be unauthorised.

Article 50

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

1. In case of credit transfers, the payment service provider of the payee shall, free of charge, at the request of the payment service provider of the payer, verify whether or not the unique identifier and the name of the payee as provided by the payer match, and shall communicate the outcome of this verification to the payment service provider of the payer. Where the unique identifier and the name of the payee do not match, the payment service provider of the payer shall notify the payer of any such discrepancy detected and shall inform the payer of the degree of that discrepancy.

2. The payment service providers shall provide the service referred to in paragraph 1 immediately after the payer provided to its payment service provider the unique identifier and the name of the payee, and before the payer is offered the possibility to authorise the credit transfer.

3. Payment service providers shall ensure that the detection and notification of a discrepancy as referred to in paragraph 1 does not prevent payers from authorising the credit transfer concerned. If the payer, after being notified about a detected discrepancy, authorises the credit transfer and the transaction is executed in accordance with the unique identifier given by the payer, that transaction shall be deemed to have been executed correctly.

4. Payment service providers shall ensure that payment service users have the right to opt out from being offered the service referred to in paragraph 1 and shall inform their payment service users of the means to express such opt-out right. Payment service providers shall ensure that payment service users that initially opted out from receiving the service referred to in paragraph 1, have the right to opt in to receive that service.

5. Payment service providers shall inform their payment service users that authorising a transaction despite a detected and notified discrepancy or that opting out from receiving the service referred to in paragraph 1 may lead to transferring the funds to a payment account not held by the payee indicated by the payer. Payment service providers shall provide that information at the same time as the notification of discrepancies or when the payment service user opts out from receiving the service referred to in paragraph 1.

6. The service referred to in paragraph 1 shall be provided with respect to payment orders placed through electronic payment initiation channels and through non-electronic payment orders involving a real-time interaction between the payer and the payment service provider of the payer.

7. The matching service referred to in paragraph 1 shall not be required where the payer did not input himself the unique identifier and the name of the payee.

8. This Article shall not apply to instant credit transfers denominated in euro falling within the scope of Regulation XXX (IPR).

Article 51

Limits and blocking of the use of the payment instrument

1. Where a specific payment instrument is used for the purposes of giving permission, the payer and the payer's payment service provider may agree on spending limits for payment transactions executed through that payment instrument. Payment service providers shall not unilaterally increase the spending limits agreed with their payment service users.

2. If agreed in the framework contract, the payment service provider may reserve the right to 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 may be unable to fulfil its liability to pay.

3. In such cases the payment service provider shall inform the payer of the blocking of the payment instrument and the 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 would compromise objectively justified security reasons or is prohibited by other relevant Union or national law.

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.

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.

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) make sure 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 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);

(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.

(f) 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 Articles 57 and 59 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 13 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 use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations under Article 52. 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.

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 reasonable grounds for suspecting fraud committed by the payer and communicates those grounds to the relevant national authority in writing.

2. Where the payer's payment service provider had reasonable grounds for suspecting fraud committed by the payer, the payer's payment service provider shall, within 10 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 no fraud has been committed by the payer;

   (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.

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. The payer may be entitled to further financial compensation from the payment service provider in accordance with the law applicable to the contract concluded between the payer and the payment service provider or the contract concluded between the payer and the payment initiation service provider, where applicable.

Article 57

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

1. The payer shall not bear any financial losses for any authorised credit transfer where the payment service provider of the payer failed, in breach of Article 50(1), to notify the payer of a detected discrepancy between the unique identifier and the name of the payee provided by the payer.

2. Within 10 business days after noting or being notified of a credit transfer transaction executed in the circumstances referred to in paragraph 1, the payment service provider shall do either of the following:

   (a) refund the payer the full amount of the authorised credit transfer;

   (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.

3. Where the payment service provider of the payee is responsible for the breach of Article 50(1) committed by the payment service provider of the payer, the payment service provider of the payee shall refund the financial damage incurred by the payment service provider of the payer.

4. The burden shall be on the payment service provider of the payer or, in the case referred to in paragraph 3, of the payee to prove that there was no breach of Article 50(1).

5. Paragraphs 1 to 4 shall not apply if the payer has acted fraudulently or if the payer opted out from receiving the verification service in accordance with Article 50(4).

6. This Article shall not apply to instant credit transfers denominated in euro falling within the scope of by Regulation XXX (IPR).

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 any financial damage caused to the payee, to the payment service provider of the payee or of the payer for their failure, within the remit of their contractual relationship, 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. Where a payment services user who is a consumer was manipulated by a third party pretending to be an employee of the consumer's payment service provider using the name or e-mail address or telephone number of that payment service provider unlawfully 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 any delay, reported the fraud to the police and notified its payment service provider.

2. Within 10 business days after noting or being notified of the fraudulent authorised payment transaction, 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 reasonable grounds 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.

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.

5. Where informed by a payment service provider of the occurrence of the type of fraud as referred to in paragraph 1, electronic communications services providers shall cooperate closely with payment service providers and act swiftly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC, including with regard to calling line identification and electronic mail address.

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 use of a lost or stolen payment instrument or from the misappropriation of a payment instrument.

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

   (a) the loss, theft or misappropriation of a payment instrument 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.

   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 subparagraph shall not apply.

   Where the payer has neither acted fraudulently nor intentionally failed to fulfil its obligations under Article 52, national competent authorities 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.

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 same shall apply 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.

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 the context of a card-based payment transaction and the exact future amount is not known at the moment when the payer authorizes 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 permission 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 the payer 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 authorised payment transactions which were initiated by a payee, including direct debits as referred to in Article 1 of Regulation (EU) No 260/2012, 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 10 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 of payment orders

1. Where the payment service provider refuses to execute a payment order or to initiate a payment transaction, the payment service provider shall notify the refusal and, if possible, the reasons for that refusal and the procedure for correcting any factual

mistakes that led to the refusal to the payment service user, unless prohibited by other relevant Union or national law.

The payment service provider shall provide or make available the notification in an agreed manner at the earliest opportunity, and in any case within the periods specified in Article 69.

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.

2. Where all of the conditions set out in the payer's framework contract are met, the payer's account servicing 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 prohibited by other relevant Union or national law.

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.

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 4 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 Article 2(1), point (c) of Regulation (EU) No 260/2012, 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. 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.

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, as far as direct debit is concerned, on the agreed due date.

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).

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.

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.

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 and 76 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 and 76. That shall include compensation where any of the payment service providers fail to apply strong customer authentication.
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 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) organizational 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[65] to:

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

   (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).

   Payment service providers shall provide to the competent authority designated under Directive (EU) XXX (PSD3) on an annual basis, or at shorter intervals as determined by the competent authority, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

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.

---

[65] 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).

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.

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.

   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 regulatory technical standards referred to in the first subparagraph in accordance with Article 15 of Regulation (EU) No 1093/2010.

Article 83

Transaction monitoring mechanisms and fraud data sharing

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

   (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) enable payment service providers to prevent and detect potentially fraudulent payment transactions, including transactions involving payment initiation services.

2. Transaction monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts online. Processing shall be limited to the following data required for the purposes referred to in paragraph 1:

(a) information on the payment service user, including the environmental and behavioural characteristics which are typical of the payment service user 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 and unique identifier of the payee;

(d) session data, including the device internet protocol address-range from which the payment account has been accessed.

Payment service providers shall not store data referred to in this paragraph longer than necessary for the purposes set out in paragraph 1, and not 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.

3. To the extent necessary to comply with paragraph 1, point (c), payment service providers may exchange the unique identifier of a payee with other payment service providers who are subject to information sharing arrangements as referred to in paragraph 5, when the payment service provider has sufficient evidence to assume that there was a fraudulent payment transaction. Sufficient evidence for sharing unique identifiers shall be assumed when at least two different payment services users who are customers of the same payment service provider have informed that a unique identifier of a payee was used to make a fraudulent credit transfer. Payment service providers shall not keep unique identifiers obtained following the information exchange referred to in this paragraph and paragraph 5 for longer than it is necessary for the purposes laid down in paragraph 1, point (c).

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

5. Payment service providers shall notify competent authorities of their participation in the information sharing arrangements referred to in paragraph 5, upon validation of their membership by participants of the information sharing arrangement or, as applicable, of the cessation of their membership, once that cessation takes effect.

6. The processing of personal data in accordance with paragraph 4 shall not lead to termination of the contractual relationship with the customer by the payment service provider or affect their future on-boarding by another payment service provider.

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.

2. Payment service providers shall organize at least annually training programmes on payment fraud risks and trends for their employees 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.

3. By [OP please insert the date= 18 months 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 with regard to the programmes on payment fraud risks referred to in paragraphs 1 and 2 of this Article.

Article 85

Strong customer authentication

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

   (a) accesses its payment account online;

   (b) accesses payment account information;

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

   (d) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2. Payment transactions that are not initiated by the payer but by the payee only shall not be subject to strong customer authentication to the extent that those transactions are initiated without any interaction or involvement of the payer.

3. 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, and where the mandate is based on an agreement between the payer and the payee for the provision of products or services, the payment transactions initiated thereafter by the payee on the basis of such a mandate may be qualified as payee initiated transactions, provided that those transactions do not need to be preceded by a specific action of the payer to trigger their initiation by the payee.

4. The payment transactions for which payment orders are placed by the payee that are based on the mandate given by the payer shall be subject to the general provisions that apply to payee-initiated transactions as referred to in Articles 61, 62 and 63.

5. Where the mandate of the payer to the payee to place payment orders for transactions referred to in paragraph 3 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 a payment service provider in the setting up of such a mandate, strong customer authentication shall be applied.

7. Payment transactions 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, shall not be subject to strong customer authentication, irrespective of whether or not the execution of the transaction is performed electronically, 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 risk involved in the service provided;

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

    (c) the payment channel used for the execution of the transaction.

12. The two or more elements referred to in Article 3, point (35), on which strong customer authentication shall be based do not necessarily need to belong to different categories, as long as their independence is fully preserved.

Article 86

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

1. Article 85(9) 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 (11).

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, unless the account servicing payment service provider has reasonable grounds to suspect fraud, but not for the subsequent access to that payment account by that account information service provider.

4. Unless the account servicing payment service provider has reasonable grounds to suspect fraud, account information service providers shall apply their own strong customer authentication when the payment services user accesses the payment account information retrieved by that account information service provider at least 180 days after strong customer authentication was last applied.

Article 87

Outsourcing agreements for the application of strong customer authentication

A payer payment service provider shall enter into an outsourcing agreement with its technical service provider in case that technical service provider is providing and verifying the elements of strong customer authentication. A payer's payment service provider shall, under such agreement, retain full liability for any failure to apply strong customer authentication and have the right to audit and control security provisions.

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.

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. Payment services providers shall develop a diversity of means for application of strong customer authentication to cater for the specific situation of all their customers.

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.

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

SECTION 1

COMPLAINT PROCEDURES

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 investigatory powers

1. Competent authorities shall exercise their powers to investigate potential infringements of this Regulation, and impose administrative sanctions and 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. Member States shall designate competent authorities to ensure and monitor effective compliance with this Regulation. Those competent authorities shall take all appropriate measures to ensure such compliance.

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 2 shall possess all investigatory powers and adequate resources necessary for the performance of their tasks.

Those powers shall include:

(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 to carry out that investigation:

(i) payment services providers;

(ii) technical service providers and payment system operators;

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

(iv) electronic communications services providers;

(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 distributors of the entities referred to in points (i), (ii) and (iii) and their branches established in the Member State concerned;

(b) the power to conduct all necessary investigations of any person referred to in points (a) (i) to (vii) 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 business premises of the legal persons or of the natural persons referred to in points (a)(i) to (vii), subject to the prior notification of the competent authorities concerned.

4. Where the law of a Member State lays down criminal sanctions applicable to infringements of this Regulation in accordance with Article 96, paragraph (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 [OP please insert the date= 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.

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 system operators 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 and with other authorities from any sector concerned as applicable to each case and 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.

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 make every possible effort to 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[66], using existing competent bodies where appropriate. ADR procedures shall be applicable to payment service providers.

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.

3. Member States shall designate a competent authority to accredit, monitor and publish the quality level of the ADR entity or entities on their territory to resolve disputes concerning rights and obligations under Titles II and III, in line with Article 18 of Directive 2013/11/EU.

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.

[66] 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).

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.

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 or circumvention of the following provisions:

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

   (b) the secure data access rules by either account servicing payment service provider or by account information service providers and payment initiation service providers laid down in of Title III, Chapter 3, without prejudice to Article 45;

   (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) and Article 59(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 5 000 000, 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 the breach, where that profit can be determined.

(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 sanctions and other type of sanctioning powers in addition to those referred to in paragraph 2 of this Article and Article 98 on periodic penalty payments.

Article 98

Periodic penalty payments

1. Competent authorities shall be entitled to impose periodic penalty payments on legal or natural persons for failure to comply with any decision, order, interim measure, request, obligation or other measure adopted 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.

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) the disadvantage resulting to the legal or natural person responsible for the breach from the duplication of criminal and administrative proceedings and sanctions for the same conduct;

(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 infringements committed 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, 97, and 98 to the case concerned to ensure the proportionality thereof.

Article 100

Right of appeal

1. The decisions taken by the competent authorities pursuant to this Regulation shall be contestable before the courts.

2. Paragraph 1 shall apply also in respect of failure 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 shall not be published.

   Competent authorities shall publish the decision and the statement referred to in the first subparagraph immediately 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 up to 5 years. Personal data contained in the publication shall be kept on the official website of the competent authority only if an annual review shows the continued need to publish that data to protect the stability of the financial markets or to ensure the effective enforcement of this Regulation, and in any event for no longer than 5 years.

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;

   (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 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 [OP please insert the date = 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 or an electronic money 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 electronic money 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 services market or on payment services or electronic money 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 electronic money services users or a threat to the orderly functioning of the payment or electronic money services 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

Article 105

Delegated acts

The Commission is empowered to adopt delegated acts in accordance with Article 106 to amend this Regulation by updating the amounts referred to in Article 58(1).

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 Article 105 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 Article 105 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 Article 105 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 5 years after the date of application 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;

   (c) the appropriateness and the impact of the rules on charges including the rules on surcharging as per Article 28;

   (d) the appropriateness and impact of the rules on prevention and redress of fraud on both unauthorised and authorised transactions.

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

2. The Commission shall, by [OP please insert the date= 3 years 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 scope of this

Regulation, with regard in particular to payment systems, payment schemes and technical service providers. Where appropriate, the Commission shall submit a legislative proposal together with that report.

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 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 Annex III 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= 18 months after the date of entry into force of this Regulation].

However, Articles 50 and 57 shall apply from [OP please insert the date= 24 months after 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 Brussels,

For the European Parliament	*For the Council*
The President	*The President*