DRAFT
COMPROMISES

Payment Services Regulation (PSR)

Draft report on the 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

21 JANUARY 2023

MAREK BELKA

(Contact person: PAWEŁ WIŚNIEWSKI)

COMPROMISES

RECITALS
COMP 1

COVERS: AM 91 (S/D), AM 2 (S/D), AM 96 (ECR), AM 99 (Renew), AM 102 (S/D), AM 4 (S/D), AM 103 (Renew), AM 5 (S/D), AM 104 (Renew), AM 105 (Renew)

FALL:

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

(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. ***At the same time, the EBA should further develop certain definitions in draft regulatory technical standards in order to take into account the constantly changing market realities and objectively adapt them to the new reality constraints.***

(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 ***for the purposes of that regulation. To avoid duplicative requirements it is important that the provisions under this Regulation clearly set out where electronic-money*** *tokens* ***should be subject to the provisions of*** this Regulation.

(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.

(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. ***As a general principle, domestic ATMs which are not considered as ATM deployers not servicing payment accounts should not charge any fees for withdrawals of cash to consumers. In addition,*** 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 ***at the initiation of a transaction for Union*** ATM withdrawals in different situations, depending on the ATM from which the payment service users withdraw cash. ***More transparency also means better information from the payment service provider as regards the currency exchange.***

(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 ***applicable*** foreign exchange reference rates issued by the ***relevant*** central bank***, and the resultant currency conversion charge shown as a monetary amount in the currency used by the customer to initiate the currency conversion***. When reference is made to 'charges' in this Regulation, it should also cover, where applicable, 'currency conversion' charges.

Recitals 52 + 53 (AMs 106, 107, 108, 109) = Surcharge Ban - discuss it

COMP 2

COVERS: AM 106 (Renew)

FALL:

(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. ***It is necessary to harmonise this approach to foster a level playing field in the Union.***

Recital 57 - DEDICATED interface - discuss it

COMP 3

COVERS: AM 6 (S/D)

FALL:

(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 ***service providers*** 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.

COMP 4

COVERS: AM 7 (S/D), AM 8 (S/D) + ask the ECR about AM 112

FALL:

(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. ***Where account information service providers or payment initiation service providers decide to access a payment account other than through the dedicated interface, they should afterwards inform the relevant competent authority and justify their decision.*** 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.

(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 ***only*** 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.

COMP 5

COVERS: AM 9 (S/D), AM 10 (S/D), AM 113 (S/D) but is connected to AM 315 (EPP), AM 316 (ECR), AM 319 (Greens)

FALL:

(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.

(65a) The EBA should develop draft regulatory technical standards setting out a standardised list of data categories of information to be disclosed on the dashboard.

(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 ***entitled "***Opinion ***of the European Banking Authority*** on obstacles under ***Article 32(3) of the RTS on SCA and CSC***". 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.

COMP 6

COVERS: AM 114 (Renew), AM 115 (Renew), AM 117 (Renew), AM 11 (S/D), AM 12 (S/D)

FALL:

(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***, or other identifier such as a fiscal number, a European unique identifier as referred to in Article 16(1), second subparagraph, of Directive (EU) 2017/1132, or an LEI, that unambiguously identify*** the payee**,** provided by the payer and, should any such discrepancies be detected, notify the payer thereof. Such services, in the countries where they exist, have had a substantial positive impact on the level of fraud and errors. Given the importance of that service for the prevention of fraud and errors, such service should be available free of charge to consumers. To avoid undue frictions or delays in the processing of the transaction, the payment service provider of the payer should provide such notification within no more than a few seconds from the moment the payer has entered the payee information. To enable the payer to decide whether to proceed with the intended transaction, the payment service provider of the payer should provide such notification before the payer authorises the transaction. Certain credit transfer initiation solutions may be available to payers allowing them to place a payment order without inserting themselves the unique identifier. Instead, such data elements are provided by the provider of that initiation 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 ***or other identifier*** 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.

(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 ***or other identifier*** 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 ***or any other proxy defined by the EBA*** 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. ***This shall be in line with Regulation (EU) 202X/... of the European Parliament and of the Council of ... amending Regulations (EU) No 260/2012 and (EU) 2021/1230***[1]***.***

(78a) The payment service provider should cooperate at all times with the payment service user in cases where any discrepancies in the payments are to be proven.

[1] ***COM(2022)546 final***

COMP 7

COVERS: AM 118 (Greens), AM 119 (Renew), AM 120 (S/D), AM 13 (S/D), AM 121 (Greens), AM 122 (Renew), AM 124 (Renew)

FALL:

(79) ***Payment service users*** should be adequately protected in the context of ***the so-called social engineering fraud, where the fraudster manipulates the*** payment ***service user in performing a certain action, such as initiating a payment transaction, or handing over their security credentials to the fraudsters***. The number ***of such type*** of 'social engineering' cases has significantly increased in recent years. 'Spoofing' cases where fraudsters pretend to be employees of a customer's payment service provider***, or a relevant entity which could reasonably be linked to a trusted source of the customer, such as a central bank or government authority,*** 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' ***or 'impersonation'*** fraud are blurring the difference that existed in Directive (EU) 2015/2366 between authorised and unauthorised transactions. The conditions under which the customer ***gave*** his or her permission ***for making a payment*** should be taken into due consideration, including by courts, to qualify a transaction as being authorised or unauthorised. ***Therefore, where the customer denies having authorised a payment, the use of the payer's personalised security credentials to authenticate a payment, including where relevant the application of strong customer authentication, should not in itself be sufficient to prove that the payment*** transaction ***was*** authorised ***by the payer. ~~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 have more means than consumers to put an end to cases ***of "spoofing", where the fraudster impersonates an employee of the payment service provider and misuses the payment service provider's name, mail address or telephone number to trick customers into carrying out some actions***, through adequate prevention and robust technical safeguards developed with electronic communications services providers such as mobile network operators, internet platforms etc***. Those electronic communications services should be obliged to cooperate with payment service providers in the fight against fraud. If they fail to do so, they should be held jointly responsible in the event of fraud***. 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, 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 ***also, where relevant, have the same level of liability as payment service providers, and*** cooperate with payment service providers with a view to preventing further occurrences of that type of fraud, including by acting promptly to ensure that appropriate organizational and technical measures are in place to safeguard the security and confidentiality of communications in accordance with Directive 2002/58/EC. Any claim ***for fraud*** against other providers, such as electronic communications services providers ***or online platforms***, for financial damage caused in the context of this type of fraud should be made in accordance with ***this Regulation***.

(81 a) Online platforms can also contribute to increasing instances of fraud. Therefore, and without prejudice to their obligations under Regulation (EU) 2022/2065, they should be held liable where fraud has arisen as a direct result of fraudsters using their platform to defraud consumers.

COMP 8

COVERS: AM 14 (S/D), AM 125 (Greens), AM 127 (ECR), AM 15 (S/D), AM 128 (Renew), AM 129 (Renew)

FALL:

(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, ***making a payment to a fraudster without having any reasonable ground for believing the payee to whom the payment was intended is legitimate, or*** 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, ***persuading the bank to lift the blockade placed after a fraud alert acting on guidance from an unfamiliar third party, or giving an unblocked smartphone to a third party***. The fact that a consumer has already received a refund from a payment service provider after having fallen victim of a ***trusted institution employee impersonation fraud, for example*** 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*.

(82a) Taking into account that the term 'gross negligence' is interpreted in very different ways across the Union, the EBA should issue guidelines on how that concept is to be interpreted for the purpose of this Regulation.

COMP 9

COVERS: AM 16 (S/D), AM 17 (S/D), AM 130 (Renew), AM 131 (S/D), AM 132 (Greens), AM 18 (S/D), AM 133 (S/D), AM 19 (S/D)

FALL:

(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. ***The spending limits should be specified in the contract between the payment service provider and the payer but can be changed.*** It should be possible to maintain or establish rules specifying an execution time shorter than 1 business day.

(97) Provision of payment services by the payment services providers may entail the processing of personal data***. It should be possible to carry out such processing only with the consent of the payment service user***. 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***, but not limited to,*** 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 ***system operators*** should also implement specific organisation measures, including training on processing such data, limiting access to special categories of data and recording such access.

(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***ant*** 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. ***Where payment service providers fail to have in place the appropriate mechanisms to prevent fraud, they should be held responsible for covering the losses of payment service users resulting from fraud.***

(100a) Member States should cooperate with payment service providers and communication services providers in order to finance education campaigns targeted at citizens on how to detect payment fraud and how to avoid becoming a victim of payment-related fraudsters. Payment service providers and communication services providers should cooperate free of charge on that issue with Member States.

COMP 10

COVERS: AM 20 (S/D), AM 134 (Greens), AM 21 (S/D), AM 22 (S/D), AM 135 (Renew), AM 23 (S/D), AM 136 (Greens)

FALL:

(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 ***obligatory***. 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.

(103a) The EBA should set up a dedicated IT platform to exchange information on fraudulent accounts.

(103b) Where a payment service provider was informed beforehand of fraudulent behaviour by an account and does not block that account, it should cover the financial losses incurred by a payment service user that is a victim of such fraud.

(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 ***a service that ensures verification of the identity of the payee. Pursuant to this Regulation, the unique identifier should be verified for all credit transfers, and not only credit transfers in euro.***

(104a) The EBA should develop Draft Regulatory Technical Standards on what identifiers - except for the IBAN - should be accepted a 'unique identifiers'.

COMP 11

COVERS: AM 137 (Renew), AM 138 (S/D), AM 24 (S/D), AM 25 (S/D), AM 140 (Renew), AM 141 (Renew), AM 142 (EPP)

FALL:

(107 a) In order for consumers to benefit from continued strong SCA, and that it remains an effective tool in the fight against fraud in electronic payments, it is appropriate that the application of SCA be risk-based and outcome-focused. In turn, the rules on SCA should provide sufficient flexibility for innovation within the payments sector, including in the development of new SCA solutions.

(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 ***by the EBA*** 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. ***At the same time, SCA should always be provided free of charge.***

(109 a) In the context of business to business (B2B) or business to government (B2G) payments, SCA should be appropriate to the risk level of such transactions, taking into account in particular the already existing controls and checks that exist among these operators. In order to reduce administrative burden, SCA should not be required for every transaction in these scenarios, and should be adapted to a risk-based approach.

(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 ***or another smart device***.

(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. ***In order to increase the use of this exemption, the draft RTS should consider additional thresholds for the transaction risk analysis exemption. Furthermore, they should consider whether it is necessary to clarify whether payment service providers should count liability only towards the payer in their fraud rates.***

COMP 12

COVERS: AM 144 (S/D), AM 26, AM 146 (Renew), AM 147 (Greens)

FALL:

(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 ***enable*** the application of strong customer authentication.

(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. ***ADR procedures should be obligatory for payment service providers.***

(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. ***Before exerting this power, the EBA should ensure that it has consulted with payment service providers or third-party providers.***

(140 a) The EBA should be granted all the necessary resources, including human resources, to fulfill their mandate under this Regulation.

COMPROMISES

ARTICLES
COMP A1

COVERS: AM 149 (Renew), AM 150 (EPP), AM 151 (S/D), AM 152 (EPP), AM 153 (Greens), AM 154 (Left), AM 27 (S/D), AM 155 (The Left), AM 156 (EPP), AM 157 (EPP), , AM 170 (EPP), AM 171 (EPP), AM 173 (Left), AM 174 (Greens), AM 28 (S/D), AM 175 (EPP), AM 159 (Greens), AM 160 (Greens), AMs 161-169 (Greens and EPP)

FALL: AM 158 (ECR), 172 (ID)

Proposal for a regulation

Article 2 – paragraph 2 – point e (new)

(e) services where cash is provided ***volunarily*** 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;

Proposal for a regulation

Article 2 – paragraph 2 – point h a (new)

(h a) payment transactions using electronic money tokens as defined in Article 3 of Regulation (EU) 2023/1114, where the payment service provider has already been authorised as a crypto-asset service provider in a Member State of the European Union for those services under Title V of that Regulation

Proposal for a regulation

Article 2 – paragraph 2 – point j – point i

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

Proposal for a regulation

Article 2 – paragraph 2 – point j – point ii

(ii) instruments which can be used only to acquire a very limited range of goods or services***, including but not limited to instruments restricted to use in business-to-business transactions***;

[MEAL VOUCHERS INCLUDED IN THE SCOPE (AM 153 Greens, AM 154 Left, AM 27 S/D, AM 155 ECR, AM 156 EPP, AM 157 EPP)]

Proposal for a regulation

Article 2 – paragraph 2 – point j – point iii

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

Recital 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 childcare vouchers or ecological vouchers. ***At the same time, while meal vouchers play a crucial role in our societies, in the future it should be made sure that they are even more commonly used than it is now, which means that operators of such schemes do not charge merchants high fees which, as a consequence, limit the acceptance of meal vouchers.***

Proposal for a regulation

Article 2 – paragraph 2 – point m

(m) payment transactions and related services between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, ***including*** the collection of ***funds as well as the execution of payments*** ***by entities belonging to the***

same group on behalf of a group by a parent undertaking or its subsidiary ~~***for onward transmission to a payment service provider.***~~

Proposal for a regulation

Article 2 – paragraph 7

7. By [OP please insert the date= one year after the date of entry into force of this Regulation], the EBA shall ***develop guidelines specifying the criteria for*** 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.

~~***The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by ... [one year from the date of entry into force of this Regulation].***~~

~~***Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.***~~

Proposal for a regulation

Article 2 – paragraph 9 a (new)

9 a. The provisions of Article 59 shall also apply to electronic communication service providers, as defined in Article 3, point (55a).

Proposal for a regulation

Article 2 – paragraph 2 – point k

~~***(k) payment transactions by a provider of electronic communications networks as defined in Article 2, point (1), of Directive (EU) 2018/1972 of the European Parliament and of the Council , or services provided in addition to electronic communications services as defined in Article 2, point (4), of that Directive to a subscriber to the network or service:***~~

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

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

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

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

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

COMP B1

COVERS: AM 176 (S/D), AM 177 (EPP), AM 29 (S/D), AM 178 (Renew), AM 182 (S/D), AM 183 (Greens), AM 184 (Left), AM 30 (S/D), AM 185 (EPP), AM 186 (Renew), AM 187 (S/D), AM 191 (Renew), AM 31 (S/D), AM 192 (Greens), AM 193 (Left), AM 194 (S/D), AM 195 (Renew), AM 32 (S/D), AM 196 (Renew), AM 197 (EPP), AM 33 S/D, AM 350 (Renew), AM 62 (S/D)

FALL: AM 179, AM 180, AM 181, AM 188, AM 189, AM 190, AM 198

Proposal for a regulation

Article 3 – paragraph 1 – point 11

(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 ***natural or legal*** person who places a payment order;

Proposal for a regulation

Article 3 – paragraph 1 – point 28

(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 ***or by the payment service provider which holds the payee payment account***, based on an instruction given by the payer;

Proposal for a regulation

Article 3 – paragraph 1 – point 30

(30) 'funds' means central bank money issued for retail use, scriptural money and electronic money ~~***tokens***~~;

Proposal for a regulation

Article 3 – paragraph 1 – point 35

(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), inherence (something the user is ***or***

~~how he behaves~~) 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;

Proposal for a regulation

Article 3 – paragraph 1 – point 36 a (new)

(36a) 'e-wallet provider' means a provider that offers consumers an interface to manage one or more payment instruments, such as payment cards, in one application without possessing at any point in time the funds to be transferred;

Proposal for a regulation

Article 3 – paragraph 1 – point 39

(39) 'unique identifier' means a combination of letters, numbers or symbols specified by the payment service provider***, or an uniquely linked proxy thereof,*** 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;

Proposal for a regulation

Article 3 – paragraph 1 – point 52

(52) 'electronic money services' means the issuance of electronic money ***~~tokens~~,*** the maintenance of payment accounts storing electronic money units, and the transfer of electronic money units;

Proposal for a regulation

Article 3 – paragraph 1 – point 53

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

Proposal for a regulation

Article 3 – paragraph 1 – point 54

(54) 'ATM deployer' means operators of automated teller machines who do not ***hold*** payment accounts.

Proposal for a regulation

Article 3 – paragraph 1 – point 55

(55) ‘payment institution providing electronic money services’ means a payment institution which provides the services of issuance of electronic money ~~*tokens*~~, 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.

Proposal for a regulation

Article 3 – paragraph 1 – point 55 a (new)

(55 a) 'electronic communications service provider' means any provider falling under the scope of:

(a) Directive (EU) 2018/1972 (European electronic communications code); or

(b) Regulation (EU) 2022/1925 (Digital Markets Act).

Proposal for a regulation

Article 3 – paragraph 1 a (new)

For the purpose of paragraph 1, point (39), the EBA, taking into account relevant market practices and different methods of identification used across the Union, shall develop draft regulatory technical standards setting out an comprehensive list of the methods that can be used as a unique identifier.

The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by ... [12 months from the date of entry into force of this Regulation].

Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

~~***Under this Regulation, the 'unique identifier' check shall be carried out for euro and non-euro transfers in the Union.***~~

COMP C1

COVERS: AM 203 (Renew), AM 34 (S/D), AM 200 (Left), AM 201 (Greens), AM 204 (EPP), AM 205 (EPP), AM 206 (Left), AM 207 (Greens), AM 208 (EPP), AM 209 (Renew), AM 210 (EPP), AM 211 (Renew), AM 35, AM 36 (S/D), AM 212 (Renew), AM 213 (Greens), AM 214 (Left), AM 215 (Renew), AM 37 (S/D), AM 217 (Renew), AM 218 (Greens), AM 219 (Left), AM 38 (S/D), AM 220 (Left), AM 221 (Greens), AM 222 (Renew), AM 223 (Renew), AM 224 (Renew), AM 39 (S/D), AM 225 (Renew), AM 226 (Greens), AM 227 (Left), AM 228 (Renew)

FALL: AM 199, AM 202, AM 216

Proposal for a regulation

Article 5 – paragraph 2

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. ***Those charges shall include any mark-up over the latest available applicable foreign exchange rate issued by the relevant central bank. The information on charges and the exchange rate shall be visible in a prominent and transparent manner prior to the authorisation of the payment transaction by the payer.***

Proposal for a regulation

Article 6 – paragraph 1

1. Where, for the use of a given payment instrument, the payee requests a charge or offers a reduction, the payee shall inform the payer thereof prior to the initiation of the payment transaction***, in a clear, transparent and accessible format.***

Proposal for a regulation

Article 6 – paragraph 2

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

Proposal for a regulation

Article 7 – paragraph 1

Natural or legal persons providing cash withdrawal services as referred to in Article 38 of Directive (EU) [PSD3] shall provide ~~***or make available***~~ ***in a transparent, distinguishable and understandable way*** **to their customers information on any charges,** ***including the exchange rate and any mark-up over the latest available applicable foreign exchange rate issued by the relevant central bank,*** ~~***before the customer carries out the at the moment of the immediately before the initiation of the provision of***~~ ***directly at the initiation of the process of*** withdrawal as well as upon receipt of the cash when the transaction is completed**.**

Proposal for a regulation

Article 8 – paragraph 3

3. Charges for information referred to in paragraph 2 shall be reasonable and ~~***in line with the payment service provider's***~~ ***proportionate in relation to the*** actual costs.

Proposal for a regulation

Article 10 – paragraph 1 – introductory part

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***~~ ***250*** or store funds that do not exceed EUR ~~***200***~~ ***250*** at any time:

Proposal for a regulation

Article 13 – paragraph 1 – introductory part

1. Payment service providers shall provide ~~***or make available***~~ ***in a transparent, distinguishable and easily understandable way*** to payment service users ***at least*** the following information and conditions:

Proposal for a regulation

Article 13 – paragraph 1 – point f

(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

as well as in real monetary value in the payer's currency. These charges shall be displayed no later than the moment the payer authorises the payment transaction;

Proposal for a regulation

Article 20 – paragraph 1 – introductory part

The payment service provider shall provide ***in a transparent, distinguishable and understandable way*** the following information and conditions to the payment service user:

Proposal for a regulation

Article 20 – paragraph 1 – point c – point ii – introductory part

(ii) all charges, if any, for ~~***domestic***~~ ***Union*** automated teller machines (ATMs) withdrawals payable by payment service users to their payment service provider at an ATM of:

Proposal for a regulation

Article 20 – paragraph 1 – point c – point ii – point 2

~~***(2) a payment service provider belonging to the same network of ATMs as the user's payment service provider;***~~

Proposal for a regulation

Article 20 – paragraph 1 – point c – point v

(v) where applicable, the estimated charges for currency conversion services in relation to a credit transfer expressed as ***a total amount in real monetary value and*** a percentage mark-up over the latest available applicable foreign exchange reference rate issued by the relevant central bank***. These charges shall be clearly displayed before the final execution of the transaction by the payer and shall be displayed in the home currency of the payer in addition to the percentage mark-up***;

COMP D1

COVERS: AM 230 (EPP), AM 234 (EPP), AM 235 (Renew), AM 236 (Renew), AM 237 (EPP), AM 239 (EPP)

FALL: AM 229, AM 231, AM 232, AM 233, AM 238, AM 240

Proposal for a regulation

Article 23 – paragraph 1

1. The payment service user may terminate the framework contract at any time, unless the parties have agreed on a ***~~period of notice~~ contract term.*** Such a ***~~period~~ term*** shall not exceed 1 month.

Proposal for a regulation

Article 23 – paragraph 6

6. Member States may provide for more favourable provisions on termination for payment service users. ***The objectives of these provisions shall be aligned with this regulation and ~~Those provisions must be fully aligned with this Regulation and its objectives and~~ must be communicated to the Commission.***

Proposal for a regulation

Article 24 – paragraph 1 – point b

(b) the charges payable by the payer ***expressed in the currency of the payment and if applicable the percentage mark up on any applicable exchange rates as compared to the mid-market rate of the central bank of issue***;

Proposal for a regulation

Article 24 – paragraph 1 – point c

(c) where applicable, a breakdown of the amounts of any charges ***before the payer executes the payment***.

Proposal for a regulation

Article 25 – paragraph 2

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.

Proposal for a regulation

Article 27 – paragraph 3

3. Member States may provide that provisions in this Title are applied to microenterprises in the same way as to consumers. ***Those provisions shall be fully aligned with this Regulation and its objectives and must be communicated to the Commission.***

Proposal for a regulation

Article 28 – paragraph 3 a (new)

Charges shall not be charged for withdrawals from a domestic automatic teller machine (ATM) when this ATM's payment service provider belongs to the same network of ATMs as the user's payment service provider;

COMP E1

COVERS: AM 241-251

DISCUSS THE ISSUE OF SURCHARGES: AM 241-AM 251

COVERS: AM 252 (Renew), AM 40 (S/D), AM 254 (Greens), AM 255 (EPP), AM 256 (Greens), AM 257 (Greens), AM 260 (EPP), AM 261 (exact with the EPP AM / from ID), AM 41 (S/D), AM 265, AM 267 (Greens), AM 268 (EPP), AM 269/270 (ID/Greens), AM 43 (S/D), AM 271 (Left), AM 272 (Greens), AM 273 (Left), AM 274-278 (Greens)

FALL: AM 42 (S/D), AM 258, AM 259, AM 262, AM 263, AM 264, AM 266, AM 279

Proposal for a regulation

Article 29 – paragraph 1 – introductory part

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 ***250***, or store funds which do not exceed EUR ***250*** at any time, payment service providers may agree with their payment service users that:

AM 253 (Greens) - EXPLAIN?

Proposal for a regulation

Article 32 – paragraph 1 – introductory part

1. A credit institution ~~***shall only may***~~ ***shall only*** refuse to open or ~~***shall only***~~ ***may*** ***shall only*** close a payment account for a payment institution for its agents or distributors or for an applicant for a license as a payment institution ***in cases where it is justified on objective, non-discriminatory and proportionate grounds, in particular*** in the following cases:

Proposal for a regulation

Article 32 – paragraph 1 – point b

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

Proposal for a regulation

Article 32 – paragraph 1 – point c

(c) insufficient information and documents ***pertaining to matters set out in this paragraph*** have been received from the applicant for an account;

Proposal for a regulation

Article 32 – paragraph 1 – point e

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

Proposal for a regulation

Article 32 – paragraph 1 – point e a (new)

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

Proposal for a regulation

Article 32 – paragraph 1 b (new)

1 b. Where a credit institution makes a decision to close a payment account in accordance with this paragraph, the account closure shall take effect on expiry of a notice period which shall not be less than 6 months. This provision shall not apply if the payment account is closed due to fraud-related reasons or reasons connected to illegal activities.

Proposal for a regulation

Article 32 – paragraph 3 a (new)

3 a. A credit institution shall also notify the national competent authority of its decision to refuse to open or to close a specific payment account. The competent authorities shall publish aggregate data on payment account refusals and closures.

Proposal for a regulation

Article 32 – paragraph 5 – subparagraph 1

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 ***and specifying the objective, non-discriminatory and proportionate grounds and situations when a credit institution is able to refuse to open or is able to close a payment account for a payment institution, its agents or distributors or for an applicant for***

a licence as a payment institution. These draft regulatory technical standards shall also develop the harmonised objectives, powers and procedure to be followed by the competent authorities in respect of appeals referred to them under paragraph 4 of this Article.

Proposal for a regulation

Article 33 – paragraph 1 a (new)

1 a. Payees must offer to payment service users at least one payment method without surcharges which does not rely on the use of a payment initiation service provider.

Proposal for a regulation

Article 33 – paragraph 2 a (new)

Without prejudice to Regulation (EU) 2016/679, payment service providers shall inform consumers in a clear and comprehensible manner when they are presented with a personalised offer that is based on automated processing of personal data.

Traders such as creditors and insurance operators shall ensure that the conditions to access their services do not discriminate against consumers legally resident in the Union on ground of their nationality or place of residence, the location of the payment account, the place of establishment of the payment service provider or the place of issue of the payment instrument within the Union or on any ground as referred to in Article 21 of the Charter of Fundamental Rights of the European Union.

Any undertaking designated as a gatekeeper, pursuant to Article 3 of Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act), shall not receive access to payment systems as account information service provider.

Account information service providers shall not be allowed to combine account information data obtained pursuant to this Regulation with other types of personal data where such combination of data may result in harmful practices such as social scoring. The European Banking Authority shall develop draft Regulatory Technical Standards limiting the combination of data obtained by account information service providers with other types of personal data. 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].

COMP F1

COVERS: AM 280 (Renew), AM 282 (Renew), AM 290 (Renew), AM 292 (Renew), AM 293 (EPP), AM 294 (Renew), AM 295 (Renew), AMs **281-283, 285, 288, 289, 291**

FALL: AM 44 (S/D), AM 284, AM 286, AM 287

Proposal for a regulation

Article 35 – paragraph 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.

Account servicing payment service providers do not have to offer a special interface if the dedicated interface is unavailable except for the interface that the account servicing payment service provider uses for authentication and communication with its users, to access payment account data as referred to in Article 38 of this Regulation.

Proposal for a regulation

Article 35 – paragraph 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 ***but shall always permit access to interfaces which allow business continuity for those providers***.

Proposal for a regulation

Article 36 – paragraph 2 – point d

(d) see, prior to initiation of the payment ~~***in the case of payment initiation service providers, at least,***~~ the unique identifier of the account, the associated names ***or other identifiers*** of the account holder and the currencies ***and the account balance*** as available to the payment service user.

Proposal for a regulation

Article 36 – paragraph 4 – point h a (new)

(h a) in the case where the account servicing payment service provider offers multiple authentication options, have the choice to decide which authentication method should be presented to the payer, taking into account the least cumbersome choice for the payer.

Proposal for a regulation

Article 36 – paragraph 4 – point h a (new)

(h a) refuse to initiate a payment transaction on justified grounds.

Proposal for a regulation

Article 36 – paragraph 5 – subparagraph 1 – point b

(b) the confirmation from the account servicing payment service provider ***as soon as possible, and not longer than 30 seconds after the authorisation by the payer,*** that the payment ***has been or*** will be executed on the basis of the information available to the account servicing payment service provider, taking into account any pre-existing payment orders that might affect the full execution of the payment order being placed.

Proposal for a regulation

Article 36 – paragraph 5 – subparagraph 2 a (new)

Where the account servicing payment service provider carries out any controls which may impact the execution of the payment, these controls shall take place prior to the confirmation of payment.

COMP G1

COVERS: AM 45 (S/D), AM 296 (The Left), AM 297 (Greens), AM 297 (Left), AM 298 (Greens), AM 46 (S/D), AM 47 (S/D), AM 299 (Greens), AM 300 (The LEfT), AM 47 (S/D), AM 301 (ECR), AM 302 (Greens), AM 303 (Left), AM 304 (Greens), AM 305 (Left), AM 48 (S/D)

FALL:

Proposal for a regulation

Article 37 – title

Data access ***~~parity between dedicated access interface and customer interface~~ for third parties***

Proposal for a regulation

Article 37 – paragraph 2

2. ***In line with Regulation 2016/679/EU [GDPR],*** account servicing payment service providers shall provide account information services providers with ***~~at least the same~~ the*** information from designated payment accounts and associated payment transactions ***made available to the payment service user when directly requesting access to the account information ~~necessary for the performance of a contract to which the data subject is party~~*** provided that this information does not include sensitive payment data.

This provision shall be subject to data minimization.

Proposal for a regulation

Article 37 – paragraph 3

3. ***In line with Regulation 2016/679/EU [GDPR],*** account servicing payment service providers shall provide payment initiation service providers with ***~~at least the same~~ the*** information ***~~on~~ necessary for*** 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 ***any update to the information, including to the payment status, shall be pushed to the payment initiation service provider via the dedicated interface in real-time*** on an ongoing basis until the payment is ***~~final~~ executed or rejected.***

This provision shall be subject to data minimization.

Proposal for a regulation

Article 37 – paragraph 3 a (new)

3 a. In accordance with Article 16 of Regulation (EU) No 1093/2010, the EBA shall develop guidelines on the implementation of this paragraph for payment initiation services and account information services.

Proposal for a regulation

Article 37 – paragraph 3 b (new)

3 b. When preparing the guidelines referred to in paragraph 3a of this Article, the EBA shall consult the European Data Protection Board established by Regulation (EU) 2016/679.

COMP H1

COVERS: (discuss AM 306 of Renew) AM 307 (Greens), AM 308 (EPP), AM 309 (Renew), AM 311 (Renew), AM 312 (Greens), AM 313 (ECR), AM 314 (Greens), AM 49 (S/D), AM 50 (S/D), AM 51 (S/D), AM 52 (S/D), AM 315 (EPP), AM 316 (ECR), AM 317, AM 53 (S/D), AM 319 (Greens), AM 320 (Greens), AM 320 (Gruffat), AM 54 (S/D), AM 318 (ECR), AM 319 (Greens), AM 321 (S/D), AM 322 (EPP)

FALL: AM 310, AM 320

Proposal for a regulation

Article 38 – paragraph 1

1. Account servicing payment service providers shall take all measures in their power to prevent unavailability ***and underperformance*** of the dedicated interface. Unavailability shall be presumed to have arisen when five consecutive requests for access to information for the provision of payment initiation services or account information services receive no response from the account servicing payment service provider's dedicated interface within 30 seconds.

Proposal for a regulation

Article 38 – paragraph 2

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 ***undue*** 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.

Proposal for a regulation

Article 40 – paragraph 2

For the purposes of point (b), where some or all of the information referred to in that point is unavailable immediately after receipt of the payment order, the account servicing payment service provider shall ensure that any information***, including but not limited to any payment status update,*** about the execution of the payment order is made available to the payment initiation service provider immediately after that information becomes available to the account servicing payment service provider.

Proposal for a regulation

Article 43 – paragraph 2 – point a – introductory part

(a) provide the payment service user***, to the extent that the information is possessed by the account servicing payment service provider,*** with an overview of each ongoing permission given for the purposes of account information services or payment initiation services, including:

Proposal for a regulation

Article 43 – paragraph 2 – point a – point v a (new)

(va) the dates on which data was accessed ~~and the type of data that was retrieved during that access.~~

Proposal for a regulation

Article 43 – paragraph 2 – point b

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

Proposal for a regulation

Article 43 – paragraph 2 – point c

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

(deletion)

Proposal for a regulation

Article 43 – paragraph 2 – point d a (new)

(d a) be consistent with the Financial Data Access Regulation's dashboards and allow data holders to manage data permissions stemming from both FIDA and this Regulation through a single dashboard upon request of the user.

Proposal for a regulation

Article 43 – paragraph 2 – point c a (new)

(c a) allow payment services users to opt-out from data sharing with third parties in a general way for all present and future data access permission requests;

Proposal for a regulation

Article 43 – paragraph 2 a (new)

2a. The EBA shall develop guidelines to specify the categories of data referred to in paragraph 2, point (a), so that the data are easily understandable for consumers.

~~***The EBA shall submit the draft regulatory technical standards referred to in the first subparagraph to the Commission by ... [one year from the date of entry into force of this Regulation].***~~

~~***Power is delegated to the Commission to supplement this Regulation by adopting the regulatory technical standards referred to in the first subparagraph of this paragraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.***~~

Proposal for a regulation

Article 43 – paragraph 2 b (new)

2b. Where, pursuant to paragraph 2, point (b), a payment services user decides to withdraw data access, the account information service provider or payment initiation service provider concerned shall:

(a) no longer use the data;

(b) withdraw the data; and

(c) erase all data received as a result of the data access permission granted by the payment services user.

The provisions stated in this paragraph point (c) shall be implemented three months after the withdrawal takes place.

Proposal for a regulation

Article 43 – paragraph 4 – introductory part

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)***~~***:***

Proposal for a regulation

Article 43 – paragraph 4 – point b – point i

(i) the purpose of the permission granted by the payment service user***, in a clear and comprehensible manner for the user***;

COMP I1

COVERS: AM 328 (EPP) ,AM 323 (Renew), AM 324 (Renew), AM 325 (EPP), AM 331 (Renew), AM 332 (Greens), AM 333 (Renew), AM 334 (EPP), AM 335 (S/D), AM 336, AM 337 (Greens), AM 57 (S/D), AM 58 (S/D), AM 338 (Greens), AM 339 (Greens), AM 59 (S/D), AM 340 (EPP)

FALL: AM 55 (S/D), AM 56 (S/D), AM 326 (S/D), AM 327, AM 329, AM 330

Proposal for a regulation

Article 44 – paragraph 1 – subparagraph 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 ***and enables a straightforward and seamless consumer experience***.

Proposal for a regulation

Article 44 – paragraph 1 – subparagraph 2 – introductory part

Prohibited obstacles shall include***, but are not limited to,*** the following:

Proposal for a regulation

Article 44 – paragraph 1 – subparagraph 2 – point a

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

(b) to (i) - stay the same

Proposal for a regulation

Article 44 – paragraph 1 – subparagraph 2 – point j

(j) imposing an account information or payment initiation journey, in a 'redirection' or 'decoupled' approach ***for*** the authentication of the payment service user ***as well as imposing*** 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;

Proposal for a regulation

Article 44 – paragraph 1 – subparagraph 2 – point l a (new)

(l a) restricting a payment initiation service provider from initiating payments from unique identifiers that are proxies for payment accounts, such as mobile phone numbers, including when such identifiers are otherwise solely made available by account servicing payment service providers to payers in a dedicated channel or system such as a mobile phone application.

Proposal for a regulation

Article 44 – paragraph 1 a (new)

1 a. Measures and instruments used by account servicing payment service providers in response to suspected fraud or to comply with Regulation (EU) 2016/679 [General Data Protection Regulation] do not constitute prohibited obstacles.

Proposal for a regulation

Article 44 – paragraph 2

2. For the activities of payment initiation services and account information services the name and the account number ***or other identifier, as defined in Article 3(39),*** of the account owner shall not constitute sensitive payment data

Proposal for a regulation

Article 45 – paragraph 2 – subparagraph 1 – point d

(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***, but only as long as strictly necessary to perform such procedures.***

Proposal for a regulation

Article 45 – paragraph 2 – subparagraph 2

~~***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.***~~

Proposal for a regulation

Article 46 – paragraph 1 – point d

(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***, including the payment initiation service provider itself,*** and that they are transmitted by the payment initiation service provider through safe and efficient channels,

Proposal for a regulation

Article 46 – paragraph 2 – point a

(a) store, ***access*** ***and use*** sensitive payment data of the payment service user;

Proposal for a regulation

Article 47 – paragraph 1 – point b

(b) ensure that the personalised security credentials of the payment service user are not accessible to other parties***, including the account information service provider itself***, 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;

Proposal for a regulation

Article 48 – paragraph 1

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 ***undue*** delay the necessary ***and adequate*** enforcement measures and impose any appropriate ***and proportionate*** sanction or, where appropriate ***and duly justified***, grant access rights in accordance with Article 38(4).

COMP J1

COVERS: AM 341 (EPP), AM 342 (Greens), AM 343 (S/D), AM 344 (Renew), AM 345 (Renew), AM 346 (ECR), AM 347 (Renew), AM 348, AM 349 (Renew) AM 350 (Renew - but in article 3, please see above), AM 351 (Renew), AM 61 (S/D), AM 63 (S/D), AM 352 (Greens), AM 353 (Renew), AM 354 (EPP), AM 355 (Greens), AM 356 (Greens), AM 68 (S/D)

FALL: AM 60 (S/D)

Proposal for a regulation

Article 49 – paragraph 1

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.

Proposal for a regulation

Article 49 – paragraph 1 a (new)

1 a. The term 'permission' in this Regulation shall not be understood as the term 'consent' under Regulation (EU) 2016/679 for which the requirements of that Regulation apply. Consent under this Regulation refers to the authorisation by the payment service user for the execution of a payment transaction or for access to account information data. This requirement is without prejudice to the application of Regulation (EU) 2016/679 and of Directive 2005/29/EC.

Proposal for a regulation

Article 49 – paragraph 5

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. ***The registered use of a valid payment instrument by the payer and the use of the payer's personalised security credentials shall be considered to be the expression of the permission to execute a payment transaction. If the required authentication has been carried out with respect to a payment transaction, and the transaction was accurately recorded, entered in the accounts, and not affected by a technical breakdown or some other deficiency of the payment service provided by the payment service provider, the payer's permission to execute the payment transaction shall be presumed to have been expressed***

until evidence demonstrating the lack of expression is collected and properly evaluated. The payment service provider shall provide to the payment service user all relevant information in cases where the granting of the permission is being questioned by the payment service user and the payment service user is gathering information to prove the lack of expression of permission to execute the transaction.

Proposal for a regulation

Article 49 – paragraph 7

7. ***At any time*** 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. 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.

Proposal for a regulation

Article 55 – paragraph 2 a (new)

2a. This Article shall be without prejudice to Article 49.

Proposal for a regulation

Article 50 – title

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

Proposal for a regulation

Article 50 – paragraph 1

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 ***or other identifier that unambiguously identifies*** the payee***, such as a fiscal number, a European unique identifier as referred to in Article 16(1), second subparagraph, of Directive (EU) 2017/1132, or an LEI*** 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 ***or other identifier that unambiguously identifies*** 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.

Proposal for a regulation

Article 50 – paragraph 4

~~***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.***~~

Proposal for a regulation

Article 50 a (new)

Article 50a

Addressing location-based payment account identifier discrimination

1. When a payer makes a credit transfer to a payee holding a payment account located within the Union, the payer shall not be required to specify the Member State in which that payment account is located, provided that payment account is reachable.

2. When a payee accepts a credit transfer or uses a direct debit to collect funds from a payer holding a payment account located within the Union, the payee shall not be required to specify the Member State in which that payment account is located, provided that payment account is reachable.

Proposal for a regulation

Article 51 – paragraph 1

1. Where a specific payment instrument is used for the purposes of giving permission, the payer's payment service provider ***shall offer to the payment service user the possibility of setting fair and proportionate*** spending limits for payment transactions executed through that payment instrument. Payment service providers shall not unilaterally ~~***increase***~~ ***change*** the spending limits agreed with their payment service users. ***By default, the spending limit set shall be at a low level and shall be specified in the contract between the payment service provider and the payer.***

Proposal for a regulation

Article 51 – paragraph 2

2. ~~***If agreed in the framework contract,***~~ The payment service provider ***shall*** block the payment instrument ***in case of*** objectively justified ***risks*** 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. ***Where such blocking does not***

take place despite reasonable grounds to suspect fraud, the payer shall not bear any financial consequences, except where the payer has acted fraudulently.

Proposal for a regulation

Article 51 – paragraph 4 a (new)

4 a. The burden of proof shall lie with the payment service provider to prove that it has complied with the requirements of this Article, if questioned by the PSU.

COMP K1

COVERS: AM 64 (S/D), AM 357 (EPP), AM 358 (Greens), AM 65 (S/D), AM 359 (S/D), AM 66 (S/D), AM 360 (Greens), AM 361 (Greens), AM 362 (Greens), AM 67 (S/D)

FALL: AM 363

Proposal for a regulation

Article 52 – paragraph 1 – point b

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

Proposal for a regulation

Article 53 – paragraph 1 – point c

(c) ensure that appropriate means, ***including free of charge ~~telephone lines~~ communication channel allowing for ~~well-qualified personal~~ human support without prior identification and in the official language of the host Member State*** are available at all times to enable the payment service user

(i) to make a notification pursuant to Article 52 point (b), or to request unblocking of the payment instrument pursuant to Article 51(4) *;*

(ii) to make a notification about a fraudulent transaction;

(iii) to receive qualified advice when suspecting to be victim of a fraud attack;

(iv) notify about problematic issues concerning conducted payments, such as errors of the payment machines during the payments.

Proposal for a regulation

Article 53 – paragraph 1 – point f a (new)

(ea) use safe communication channels and, in principle, refrain from sending links and documents via e-mail;

Proposal for a regulation

Article 53 – paragraph 2 a (new)

2a. Where the payer's payment service provider does not comply with the obligations set out in this Article, the payer shall not bear any resulting financial losses unless the payer acted with gross negligence or fraudulently.

The burden of proof shall lie on the payment service provider to prove that it complied with this Article.

ARTICLE 55 - POLITICAL!

COMP L1

COVERS: AM 69 (S/D), AM 374 (EPP), AM 375(EPP), AM 376 (EPP), AM 377 (EPP), AM 378-9 (Greens), AM 70 (S/D), AM 382 (EPP), AM 383 (EPP), AM 384 (Greens), AM 385 (Greens), AM 386 (EPP), AM 387 (Greens)

FALL: AM 380, AM 381

Proposal for a regulation

Article 56 – paragraph 1

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 ~~***gross negligence or***~~ fraud committed by the payer and communicates those grounds to the relevant national authority in writing.

Proposal for a regulation

Article 56 – paragraph 2 – introductory part

2. Where the payer's payment service provider had reasonable grounds for suspecting ~~***gross negligence or***~~ 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:

Proposal for a regulation

Article 56 – paragraph 2 – point a

(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 ~~***gross negligence or***~~ fraud has been committed by the payer;

Proposal for a regulation

Article 56 – paragraph 2 – point b

(b) provide a justification ***to the relevant national authority and to the payer*** for refusing the refund~~***, provide proof that the payer acted fraudulently or with gross negligence***~~ 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.

Proposal for a regulation

Article 57 – paragraph 2 – introductory part

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:

Proposal for a regulation

Article 57 – paragraph 2 – point b

(b) provide ***an accurate*** ***and substantiated*** justification ***to the payer in writing*** for refusing the refund***, provide proof to the relevant competent authority that there was no infringement of Article 50(1)*** 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.

Proposal for a regulation

Article 57 – paragraph 5

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

Proposal for a regulation

Article 57 – paragraph 5 a (new)

5 a. The burden of proof shall be on the payment service providers to prove that the payer has acted fraudulently or with gross negligence

COMP M1

COVERS: AM 389 (ECR), AM 390 (Greens), AM 71 (S/D), AM 392 (EPP), AM 393 (EPP), AM 72 (S/D), AM 394 (Renew), AM 395 (EPP), AM 396 (ECR), AM 397 (EPP), AM 399 (Renew), AM 400 (Greens), AM 401 (The Left), AM 402 (EPP), AM 405 (ECR), AM 406 (Renew), AM 407 (ECR), AM 410 (Greens), AM 411 (The Left), AM 412 (Renew/EPP), AM 413 (ECR), AM 415 (ECR), AM 416 (Renew), AM 417 (EPP), AM 418 (Renew), AM 73 (S/D), AM 420 (Renew), AM 74 (S/D), AM 421 (EPP), AM 422 (The Left), AM 423 (EPP), AM 426 (Renew), AM 429 (Greens)

FALL: AM 388, AM 391, AM 398, AM 403, AM 404, AM 408, AM 409, AM 414, AM 419, AM 424, AM 425

Proposal for a regulation

Article 58 – paragraph 1

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

Proposal for a regulation

Article 59 – title

~~***Payment service provider's liability for***~~ Impersonation fraud

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 ***or any other relevant entity of public or private nature*** using the name or e-mail address or telephone number of that ~~***payment service provider***~~ ***entity*** 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. ***Upon the receipt of the notification, payment service providers shall inform the consumer if a report of the fraud case to the police is required to further process the consumer's claim.***

2. Within 10 business days after ~~***noting or***~~ being notified of the fraudulent authorised payment transaction ***by the consumer and being presented with the police report***, 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 ***the relevant documents to the relevant national authority that the consumer has acted fraudulently or with gross negligence and a substantiated*** 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 ***or refuses to comply with the PSP's investigation, providing relevant information on the circumstances of the impersonation***.

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. ***If the electronic communications services providers do not remove the fraudelant or illegal content, after being informed, they 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.***

5a. Electronic communications service providers shall have in place all necessary educational measures, including alerts to their customers via all appropriate means and media when new forms of online scams emerge, taking into account the needs of their most vulnerable groups of customers.

Electronic communications service providers shall give their customers clear indications as to how to identify fraudulent attempts and warn them as to the necessary actions and precautions to be taken to avoid falling victim to fraudulent actions targeting them. Electronic communications service providers shall inform their customers of the procedure for reporting fraudulent actions and how to rapidly obtain fraud-related information.

5 b ***By [12 months after the entry in force of this Regulation], EBA shall issue technical guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 regarding the***

concept of gross negligence in the context of this Regulation and respecting the national legal frameworks on this matter.

COMP N1

COVERS: AM 78 (S/D), AM 427 (Greens), AM 76 (S/D), AM 428 (Greens), AM 430 (EPP), AM 434 (EPP), AM 435 (EPP), AM 436 (EPP), AM 437 (EPP), AM 438 (EPP), AM 439 (EPP), AM 440 (EPP), AM 441 (EPP), AM 442 (EPP), AM 443 (EPP)

FALL: AM 431, AM 432, AM 433

Proposal for a regulation

Article 60 – paragraph 1 – subparagraph 2 – point a

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

Proposal for a regulation

Article 60 – paragraph 1 a (new)

~~***1a. Where the payer's payment service provider has reasonable grounds to suspect fraud or gross negligence by the consumer, within 10 business days after noting or being notified of the fraudulent authorised payment transaction, the payment service provider shall do one of the following:***~~

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

~~***(b) provide proof that the consumer has acted fraudulently or with gross negligence to the relevant national authority and provide to the payer a substantiated justification for refusing the refund and indicate to the consumer the bodies to which the consumer can refer the matter in accordance with Articles 90, 91, 93, 94 and 95 if the consumer does not accept the reasons provided.***~~

Proposal for a regulation

Article 61 – paragraph 1

1. Where a payment transaction is initiated by or through the payee in the context of a card-based payment transaction***, an account-to-account based transaction or a credit transfer*** 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.

Proposal for a regulation

Article 65 – paragraph 1 – subparagraph 2

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. ***Where the PSP refuses to execute the payment based on objective grounds to suspect a fraudulent payment transaction in accordance with Article 83(1), the notification shall take into account the information necessary for the payment service user to resolve the suspicious transaction.***

Proposal for a regulation

Article 65 – paragraph 1 – subparagraph 3

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

Proposal for a regulation

Article 68 – paragraph 2

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

Proposal for a regulation

Article 69 – paragraph 2 a (new)

2 a. Where the transaction monitoring mechanisms according to Article 83(1) provide reasonable grounds to suspect a fraudulent payment transaction, the payee's payment service provider may refuse to make the funds immediately available to the payee's payment account. The payee's payment service provider shall, as appropriate and without undue delay, seek clarification on the suspected fraud payment transaction and, depending on that outcome, either make the funds available or return them to the payer's account servicing payment service provider.

Proposal for a regulation

Article 69 – paragraph 3

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. ***Paragraph [2a new] applies accordingly.***

Proposal for a regulation

Article 72 – paragraph 1

For national payment transactions, Member States may provide for shorter maximum execution times than those provided for in this Section. ***Decisions taken under this Article must be communicated to the Commission.***

Proposal for a regulation

Article 74 – paragraph 4

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

COMP O1

COVERS: AM 444 (S/D), AM 445 (Renew), AM 446 (Greens), AM 450 (Greens), AM 81 (S/D), AM 451 (Greens), AM 82 (S/D), AM 452 (Greens), AM 453 (Greens)

FALL: AM 79 (S/D), AM 80 (S/D), AM 447, AM 448, AM 449

Proposal for a regulation

Article 80

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, ***including for the prevention, investigation and detection of payment fraud***, 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.

~~***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 when necessary for the prevention, investigation and detection of payment fraud, subject to appropriate safeguards for the fundamental rights and freedoms of natural persons, on the basis that such prevention, investigation and detection is a substantial public interest as referred to in Article 9(2), point (g), of Regulation (EU) 2016/679 and on the basis of Article 6(1), points (c) and (d) of Regulation (EU) 2016/679. Without prejudice to the above, payment service providers shall only access, retain and process personal data necessary for the provision of payment services.*** Payment systems, payment service providers and ***technical 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 ***or in order to ensure the optimal performance of inherence-based strong customer authentication or*** 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:~~

Proposal for a regulation

Article 81 – paragraph 1 – subparagraph 1

Payment service ***providers and e-wallet*** 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.

Proposal for a regulation

Article 81 – paragraph 1 – subparagraph 2 – point b

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

Proposal for a regulation

Article 82 – paragraph 1 – subparagraph 1 (new)

Statistical data sets on fraud shall include the number and value of reimbursed fraudulent transactions. Where reimbursement has been refused, payment service providers shall provide the reason for the rejection such as stipulating that the consumer has acted fraudulently or with gross negligence.

Proposal for a regulation

Article 82 – paragraph 1 a (new)

1 a. National competent authorities, the European Banking Authority and the European Central Bank shall publish the statistical data in aggregated form at least on a yearly basis.

COMP P1

COVERS: AM 454 (ECR), AM 455 (ECR), AM 456 (Renew), AM 457 (Renew), AM 458 (EPP), AM 459 (Renew), AM 83 (Rapporteur), AM 460 (EPP), AM 461 (ECR), AM 462 (Renew), AM 463 (Renew/EPP), AM 464 (EPP), AM 465 (ECR), AM 467 (ECR), AM 468 (Renew), AM 469 (EPP), AM 470 (Greens), AM 471 (The Left), AM 472 (EPP), AM 473 (EPP), AM 474 (Renew), AM 475 (EPP), AM 476 (EPP), AM 477 (The Left), AM 478 (Greens), AM 479 (Renew), AM 480 (EPP), AM 84 (Rapporteur), AM 481 (The Left), AM 482 (Greens), AM 483 (Renew), AM 484 (EPP), AM 85 (Rapporteur), AM 485 (The Left), AM 486 (Greens), AM 487 (Greens), AM 488 (The Left), AM 489 (The Left), AM 490 (EPP), AM 491 (Renew/EPP), AM 492 (Greens)

FALL: ~~AM 460~~, AM 466

Proposal for a regulation

Article 83 – title

Fraud monitoring mechanisms and fraud data sharing

Proposal for a regulation

Article 83 – paragraph 1 – introductory part

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

Proposal for a regulation

Article 83 – paragraph 1 – point a

(a) support the ~~***risk-based***~~ application of strong customer authentication in accordance with Article 85;

Proposal for a regulation

Article 83 – paragraph 1 – point b

(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***, including through the transaction monitoring mechanisms as outlined in paragraph 2 of this Article***;

Proposal for a regulation

Article 83 – paragraph 1 – point c

(c) ~~*enable payment service providers to*~~ prevent, detect ***and - if possible - resolve*** potentially fraudulent payment transactions, including transactions involving payment initiation services.

Proposal for a regulation

Article 83 – paragraph 2 – subparagraph 1 – introductory part

~~Transaction~~ ***Fraud*** monitoring mechanisms shall be based on the analysis of previous payment transactions and access to payment accounts ***online as well as on the fraud data shared and observed fraud patterns***. Processing shall ***include*** the following data required for the purposes referred to in paragraph 1:

Proposal for a regulation

Article 83 – paragraph 2 – subparagraph 1 a (new)

When the monitoring mechanisms provide strong evidence to suspect a fraudulent transaction, or when a police report is notified by the user to the payment service provider, payment service providers shall have the right to block the execution of the payment order, or block and recover the related funds. That evidence should be understood as objectively justified reasons relating to the security of the payment transaction, the suspicion of unauthorised or fraudulent transactions.

This article is subject to the data minimization principle and GDPR.

Proposal for a regulation

Article 83 – paragraph 2 – subparagraph 1 b (new)

Payees' payments service providers shall provide the data required for the purposes referred to in paragraph 1 to the payment service providers involved in the transaction.

Proposal for a regulation

Article 83 – paragraph 2 – subparagraph 2 a (new)

Payment service providers may process the data listed in the first subparagraph of Article 83(2) for strong customer authentication as an element of 'inherence' pursuant to Article 3, point (35).

Proposal for a regulation

Article 83 – paragraph 3

3. To comply with paragraph 1, point (c), payment service providers ***shall*** exchange the unique identifier, ***name, personal identification number, organisation number, modus operandi and other transaction information*** of a payee with other payment service providers who are subject to inform ation 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 ***information*** shall be assumed when at least two different payment services users who are customers of the same payment service provider ***or a consumer organization*** have informed that a unique identifier of a payee was used to make a fraudulent credit transfer. Payment service providers shall not keep ***information*** 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).

Proposal for a regulation

Article 83 – paragraph 3 a (new)

3 a. To the extent necessary to comply with paragraph 1, point (c), payment service providers, law enforcement agents and public authorities may also exchange the information referred to in paragraph 3 with public authorities.

Proposal for a regulation

Article 83 – paragraph 4

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, ***if applicable***. 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. ***The information sharing arrangements shall be concluded by [OP please insert the date = 12 months after the date of entry into force of this Regulation].***

Proposal for a regulation

Article 83 – paragraph 4 a (new)

4a. The EBA shall set up a dedicated IT platform to allow payment service providers to exchange information on fraudulent unique identifiers and other relevant information described in this Article with other payment service providers.

That platform shall be set up by ... [12 months from the date of entry into force of this Regulation].

Proposal for a regulation

Article 83 – paragraph 5

5. Payment service providers shall notify competent authorities of their participation in the information sharing arrangements referred to in paragraph ***4***, 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.

Proposal for a regulation

Article 83 – paragraph 5 a (new)

5a. Where the payment service provider fails to block a unique identifier which was reported to that payment service provider as fraudulent or involved in transactions demonstrably confirmed as fraudulent, the payment service user shall not bear any resulting financial losses.

Proposal for a regulation

Article 83 – paragraph 5 b (new)

5 b. Where payment fraud originates in the publication of fraudulent content online, payment service providers shall, without undue delay, inform providers of hosting services following the procedure laid down in Article 16 of Regulation (EU) 2022/2065 [Digital Services Act].

Proposal for a regulation

Article 83 – paragraph 5 c (new)

5 c. The payment service providers shall be responsible to provide evidence on whether the IBAN has been proven to be fraudulent.

Proposal for a regulation

Article 83 – paragraph 6

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 ***unless a thorough fraud investigation conducted by the relevant authorities has concluded that the customer participated in the fraudulent activity***.

Proposal for a regulation

Article 83 – paragraph 6 a (new)

6 a. The burden of proof shall lie with the payment service providers to prove that they have complied with the requirements under this article.

COMP Q1

COVERS: AM 494 (EPP), AM 495 (Greens), AM 77 (S/D), AM 493 (Renew), AM 496 (Renew), AM 500 (S/D), AM 501 (EPP), AM 505 (S/D), AM 506 (Renew), AM 507 (Renew), AM 511 (EPP), AM 512 (EPP), AM 514 (ECR), AM 515 (S/D), AM 516 (Renew), AM 517 (Greens), AM 518 (EPP)

FALL: AM 497, AM 498, AM 499, AM 502, AM 503, AM 504, AMs 508-510, AM 513, AM 519

Proposal for a regulation

Article 84 – paragraph 2

2. Payment service providers shall organize at least annually training programmes on payment fraud risks and trends for their employees ***active in designing and maintaining payment services and offering them to customers*** 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.

Proposal for a regulation

Article 84 – paragraph 1a (new)

Member States shall allocate substantial means to invest in education on payment-related fraud. Such education may take the form of a media campaign or lessons at schools. Payment service providers and electronic communications service providers shall cooperate free of charge with the Member States in those educational activities. Member States shall inform the Parliament and the Commission ~~and the EBA~~ about the planned campaigns.

Payment service providers, in cooperation with electronic communications services providers, shall take adequate prevention and robust technical safeguards to prevent cases where fraudsters replicate and misuse the payment service provider's name, mail address or telephone number for misleading payment service users into making fraudulent transactions.

Electronic communications services providers shall cooperate with payment service providers 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.

Proposal for a regulation

Article 85 – paragraph 1 – introductory part

1. A payment service provider shall apply strong customer authentication***, on the basis of the risk assessment carried out under transaction monitoring mechanism as set out in Article 83,*** where the payer:

Proposal for a regulation

Article 85 – paragraph 1 a (new)

~~***1 a. Payers should not experience strong customer authentication more than once in a single customer journey if the trust it creates can be reused by involved parties without being detrimental to security, data protection or consumer rights.***~~

Proposal for a regulation

Article 85 – paragraph 2

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. ***Such exemptions shall also apply to refunds that are initiated by the original payee in favour of the payer.***

Proposal for a regulation

Article 85 – paragraph 7

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-based mechanisms***, 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 ***another form than strong customer authentication for*** authentication of the payment transaction. ***The possible forms of authentication in such cases shall be described by the national competent authority.***

Proposal for a regulation

Article 85 – paragraph 11 – introductory part

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

Proposal for a regulation

Article 85 – paragraph 11 – point c a (new)

(c a) whether the parties performing the transaction are consumers or corporate payers.

Proposal for a regulation

Article 85 – paragraph 12

12. The two or more elements referred to in Article 3, point (35), on which strong customer authentication shall be based need to belong to different categories~~, except when they are based on the inherence category~~. *Always the* independence *of the elements shall be* fully preserved and *the authentication procedure ensures a high level of security. Payment service providers shall not use two elements categorised as knowledge.*

The inherence element of strong customer authentication may include environmental and behavioural characteristics such as those related to the location of the payment service user, time of transaction or the device being used.

COMP R1

COVERS: AM 253, AM 520 (S/D - technical), AM 525 (ECR), AM 526 (Renew), AM 527 (EPP), AM 531 (Renew), AM 532 (Greens), AM 533 (EPP), AM 534 (Greens), AM 87 (S/D), AM 88 (S/D), AM 535 (EPP), AM 537 (EPP)

FALL: AM 521, AM 522, AM 523, AM 524, AM 528, AM 529, AM 530, AM 536

Proposal for a regulation

Article 86 – paragraph 1

1. Article ***85(8) and (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.

Article 86 – paragraph 4

~~***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.***~~

Proposal for a regulation

Article 87 – paragraph 1

A payer payment service provider shall ***comply with the existing EBA guidelines on*** outsourcing ***arrangements (EBA/GL/2019/02) in case*** its technical service provider ***is carrying out*** strong customer authentication ***on an outsourced basis on behalf of the payment service provider. In such circumstances,*** a payer's payment service provider shall retain full liability for any failure to apply strong customer authentication and have the right to audit and control security provisions.

Proposal for a regulation

Article 88 – paragraph 2

2. Payment services providers shall not make the performance of strong customer authentication dependant on the exclusive use of a single means of authentication and shall not make the performance of strong customer authentication depend, explicitly or implicitly, on the possession of a smartphone ***or other smart device***. Payment services providers shall develop ***more than one mean for the application of*** ~~**diversity of means for application of**~~ strong customer authentication to cater for the ***various*** situation of all their customers, ***specifically those with disabilities, low digital skills, older persons and those who do not have access to digital channels or payment instruments.***

Proposal for a regulation

Article 88 – paragraph 2 a (new)

2 a. All means of authentication shall be provided free of charge.

Proposal for a regulation

Article 88 a (new)

Article 88a

Fair, reasonable and non-discriminatory access to mobile devices

1. Without prejudice to Article 6 paragraph (7) of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, original equipment manufacturers of mobile devices and providers of electronic communication services within the meaning of Article 2 (1) Directive (EU) 2018/1972 shall allow providers of front end services effective interoperability with, and access for the purposes of interoperability to, the technical features necessary for storing and transferring data to process payment transactions, on fair, reasonable and non-discriminatory terms.

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

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

Proposal for a regulation

Article 89 – paragraph 1 – subparagraph 1 – point d

(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. ***When doing so, the EBA shall take into account its existing guidelines on outsourcing arrangements.***

COMP S1

COVERS: AM 538 (EPP), 539 (ECR), AM 540 (EPP), AM 541 (EPP), AM 542 (Renew), AM 543 (Renew), AM 545 (S/D/Greens/Renew), AM 546 (S/D/Greens/Renew), AM 547 (Greens), AM 89 (Rapporteur), AM 90 (Rapporteur), AM 548 (Greens), AM 552 (Greens), AM 553, AM 554 (S/D - technical), AM 557 (ECR), AM 558 (ECR), AM 559 (ECR), AM 560 (ECR)

FALL: AM 544, AM 549, AM 550, AM 551, AM 555, AM 556, AM 561, AM 562, AM 563, AM 564, AM 565, AM 566, AM 567, AM 568, AM 569

Proposal for a regulation

Article 89 – paragraph 1 – subparagraph 2 – point i

(i) the conditions that have to be met for a remote electronic payment transaction to be considered as posing a low level of risk***, taking into consideration the levels of fraud in each economic activity***;

ga (new)

standardised list of data categories of information to be disclosed on the dashboard.

an exhaustive list of the methods that can be used as a unique identifier.

the criteria for 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 2.

Proposal for a regulation

Article 89 – paragraph 2 – subparagraph 1 a (new)

The EBA, before submitting its draft regulatory technical standards to the Commission, shall have an open consultation with public and private stakeholders in order to ensure that the most up to date advances in technology and payment processing, as well as the specificities of business to business and business to government transactions are taken into account in the draft regulatory technical standards.

Proposal for a regulation

Article 89 – paragraph 2 – subparagraph 1 – point e a (new)

(e a) the need for balance between fraud risk versus the consumer experience with regards to low value transactions.

Proposal for a regulation

Article 89 – paragraph 2 – subparagraph 1 – point e b (new)

(e b) the different situation and specific needs of consumer and corporate payers.

Proposal for a regulation

Article 92 – paragraph 1

1. Without prejudice to cases covered by national criminal ~~***or tax***~~ 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.

Proposal for a regulation

Article 93 – paragraph 4

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. ~~***Article 92(1) shall not preclude the exchange of information between competent authorities and tax authorities in the same Member State. Where the information originates in another Member State, it shall only be disclosed in accordance with the first sentence of this subparagraph with the express agreement of the competent authorities which have disclosed it.***~~

Proposal for a regulation

Article 94 – paragraph 2 – subparagraph 1

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.

Proposal for a regulation

Article 95 – paragraph 1 a (new)

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

Proposal for a regulation

Article 99 a (new)

Consumers shall have access to proportionate and effective remedies, including compensation for damage suffered by the consumer. Those remedies shall be without prejudice to the application of other remedies available to consumers under Union or national law.

~~***In the event of failure by the payment service provider to comply with the rules laid down in this Regulation, the amounts due shall bear interest at the statutory rate plus five percentage points. If the payment is more than seven days late, the amount due shall bear interest at the statutory rate plus ten percentage points. If the payment is more than 30 days late, the amount due shall bear interest at the statutory rate plus 15 percentage points.***~~

Proposal for a regulation

Article 104 a (new)

Article 104a

Product intervention by competent authorities

1. A competent authority may prohibit or restrict a certain type or a specific feature of a payment service or instrument or an electronic money service.

2. A competent authority may take the action referred to in paragraph 1 if it is satisfied on reasonable grounds that:

(a) the proposed action addresses a significant number of payment services users or holders of electronic money 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) the action is proportionate taking into account the nature of the risks identified and the likely effect of the action on payment services users or holders of electronic money who may use or benefit from the payment or electronic money service;

(d) the competent authority has properly consulted competent authorities in other Member States that may be significantly affected by the action;

(e) the action does not have a discriminatory effect on services or activities provided from another Member State.

3. Where the conditions set out in the first subparagraph are fulfilled, the competent authority 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 marketed, distributed or sold to clients.

A prohibition or restriction may apply in circumstances, or be subject to exceptions, specified by the competent authority.

4. The competent authority shall not impose a prohibition or restriction under this Article unless, not less than one month before the measure is intended to take effect, it has notified all other competent authorities and EBA in writing or through another medium agreed between the authorities the details of:

(a) the payment service or electronic money service to which the proposed action relates;

(b) the precise nature of the proposed prohibition or restriction and when it is intended to take effect; and

(c) the evidence upon which it has based its decision and upon which it is satisfied that each of the conditions in paragraph 2 are met.

5. In exceptional cases where the competent authority deems it necessary to take urgent action under this Article in order to prevent detriment arising from the payment service or electronic money service referred to in paragraph 1, the competent authority may take action on a provisional basis with no less than 24 hours' written notice, before the measure is intended to take effect, to all other competent authorities and EBA, provided that all the criteria in this Article are met and that, in addition, it is clearly established that a one month notification period would not adequately address the specific concern or threat. The competent authority shall not take action on a provisional basis for a period exceeding three months.

6. The competent authority shall publish on its website notice of any decision to impose any prohibition or restriction referred to in paragraph 1. The notice shall specify details of the prohibition or restriction, a time after the publication of the notice from which the measures will take effect and the evidence upon which it is satisfied each of the conditions in paragraph 2 are met. The prohibition or restriction shall only apply in relation to actions taken after the publication of the notice

7. The competent authority shall revoke a prohibition or restriction if the conditions in paragraph 2 no longer apply.

8. The Commission shall adopt delegated acts in accordance with Article 50 specifying criteria and factors to be taken into account by competent authorities in determining when there is a significant consumer protection concern or a threat to the orderly functioning and integrity of the payment and electronic money markets for the purposes of paragraph 2, first subparagraph, point (a). Those criteria and factors shall include:

(a) the degree of complexity of a payment or electronic money service and the relation to the type of user to whom it is marketed, distributed and sold;

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

Proposal for a regulation

Article 105 – paragraph 1

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 ***60(1).***

Proposal for a regulation

Article 108 – paragraph 1 – subparagraph 1 – point d a (new)

(d a) the number and the amount of administrative penalties and administrative measures imposed according to or in relation to this Regulation, categorised by Member State;

Proposal for a regulation

Article 108 – paragraph 1 – subparagraph 1 – point d b (new)

(d b) the quality of cooperation between national competent authorities and EBA;

Proposal for a regulation

Article 108 – paragraph 1 – subparagraph 1 – point d c (new)

(d c) types and trends of fraudulent behaviour, and estimations and proportions of financial damage that behaviour represents on the market, quantified by Member States;