



Brussels, 27.11.2017  
C(2017) 7782 final

**COMMISSION DELEGATED REGULATION (EU) No .../..**

**of **XXX****

**supplementing Directive 2015/2366 of the European Parliament and of the Council with  
regard to regulatory technical standards for strong customer authentication and  
common and secure open standards of communication**

(Text with EEA relevance)

## **EXPLANATORY MEMORANDUM**

### **1. CONTEXT OF THE DELEGATED ACT**

Article 98(4) of Directive (EU) No 2015/2366 empowers the Commission to adopt, following submission of draft standards by the European Banking Authority (EBA), and in accordance with Articles 10 to 14 of Regulation No (EU) 1093/2010, delegated acts specifying the requirements of the strong customer authentication, the exemptions from its application and common and secure open standards of communication.

In accordance with Article 10(1) of Regulation No (EU) 1093/2010 establishing the EBA, the Commission shall decide within three months of receipt of the draft standards whether to endorse the drafts submitted. The Commission may also endorse the draft standards in part only, or with amendments, where the Union's interests so require, having regard to the specific procedure laid down in those Articles.

### **2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT**

In accordance with the third subparagraph of Article 10(1) of Regulation No (EU) 1093/2010, the EBA has carried out a public consultation on the draft technical standards submitted to the Commission in accordance with Article 98(4) of Directive (EU) No 2015/2366. A consultation paper was published on the EBA internet site on 12 August 2016, and the consultation closed on 12 October 2016. Moreover, the EBA invited the EBA's Banking Stakeholder Group set up in accordance with Article 37 of Regulation No (EU) 1093/2010 to provide advice on them. Together with the draft technical standards, the EBA has submitted an explanation on how the outcome of these consultations has been taken into account in the development of the final draft technical standards submitted to the Commission.

Together with the draft technical standards, and in accordance with the third subparagraph of Article 10(1) of Regulation No (EU) 1093/2010, the EBA has submitted its Impact Assessment, including its analysis of the costs and benefits, related to the draft technical standards submitted to the Commission. This analysis is available at <https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf>, pages 40-44 of the Final Draft Regulatory Technical Standards package.

### **3. LEGAL ELEMENTS OF THE DELEGATED ACT**

These Regulatory Technical Standards (RTS) specify the requirements, under Article 98 of Directive (EU) No 2015/2366 (PSD2), of the strong customer authentication (SCA), the exemptions from the application of SCA, the requirements with which security measures have to comply in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials, and the requirements for common and secure open standards of communication (CSC) between account servicing payment service providers (ASPSPs), payment initiation service providers (PISPs), account information service providers (AISPs), payers, payees and other payment service providers (PSPs).

These RTS take into account the various objectives of PSD2, including enhancing security, promoting competition, ensuring technology and business-model neutrality, contributing to the integration of payments in the EU, protecting consumers, facilitating innovation and enhancing customer convenience.

The RTS are technology and business-model neutral. The RTS contain a number of exemptions, including two exemptions for remote payments, one on transaction-risk analysis

and the other on low value payments (below EUR 30). It also contains exemptions for proximity payments. Considering the fact that the exemption based on transaction risk analysis is based on the observance of pre-set reference fraud rates, it is appropriate that the adequacy of the fraud level monitoring mechanism(s) of the payment service provider is scrutinized by a statutory auditor to ensure an impartial assessment of the correctness of the data. The actually achieved fraud levels should not only be reported to the competent authorities, for the purpose of ensuring an effective enforcement of the exemptions; they should also be reported directly to EBA enabling it to conduct a review of the reference fraud rates in the RTS within 18 months after the RTS enters into force.

The Commission has added a further exemption from strong customer authentication in relation to EBA's proposal, covering electronic payment transactions that are performed through dedicated payment processes or protocols typically used by corporates and where security is achieved through other means than the authentication of a particular individual. This exemption is subject to competent authorities being satisfied that such payment methods achieve the high level of security of payments aimed for by PSD2.

Due to their very nature, payments made through the use of an anonymous payment instruments are not subject to the obligation of strong customer authentication. It goes without saying that where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from PSD2 and this Regulatory Technical Standard.

The RTS also establish requirements on the communication between ASPSPs, AISP and PISPs, among which the obligation for the ASPSPs to offer at least one interface for AISP and PISP for access to payment account information. With regard to the communication between ASPSPs, AISP and PISP, accordingly, the existing practice of third-party access without identification referred to in market jargon as 'screen scraping' or, mistakenly, as 'direct access' will no longer be allowed once the transition period under Article 115(4) PSD2 has elapsed and the RTS apply. However, the RTS establish requirements for ASPSPs to develop and maintain a communication interface to allow PISP, AISP and payment service providers issuing card-based payment instruments to access the data they need in compliance with PSD2. The RTS only apply to payment accounts, in accordance with the scope of PSD2. The RTS thus does not cover the access to accounts other than payment accounts, which falls under the competence of the Member States.

Where the ASPSP decides to use a dedicated interface, the RTS mandates that it shall define transparent key performance indicators and service level targets for the interface. These must be at least as stringent as those set for the interface used by the ASPSP's payment service users. In addition, it shall publish the data on a quarterly basis.

In order to guarantee that an unavailability or inadequate performance of the dedicated interface does not prevent payment initiation services and account information services providers from offering their services to the users, while at the same time the user-facing interfaces operate without any difficulties and allow the ASPSP to offer its own payment services, the Commission amended EBA's draft RTS to introduce a contingency measure in the form of a fall-back mechanism which consists in opening the user-facing interfaces as a secure communication channel for payment initiation services and account information services providers. The relevant provisions of PSD2 (Articles 65-67) apply for payment initiation services and account information services providers, including identification and authentication procedures, when using this contingency measure. Its use must be fully documented and reported to the authorities by the relevant providers, upon request.

EBA rejected in its opinion on the Commission amendments this fall-back mechanism on two main arguments: the first one related to the cost of the fall-back mechanism which would have to be borne by ASPSPs in addition to the cost of a well-functioning dedicated interfaces; secondly, EBA expressed concern that the requirement for a fall-back mechanism would weaken incentives to develop standardised dedicated interfaces, as the fall-back mechanism alone would already be sufficient for ASPSPs to comply with the requirements of PSD2.

In the light of EBA's opinion, the Commission reviewed its amendments to the RTS, maintaining the fall-back mechanism as a general principle, but empowering national competent authorities to exempt banks from having to provide it when strict conditions are met, ensuring that the dedicated interfaces genuinely open the market for payment services. Thus, dedicated interfaces shall be tested by the payment service providers who will use them, and they will be stress-tested and monitored by competent authorities. In the event that those dedicated interfaces do not succeed in the testing phases or fail the stress test, payment service providers will be able to use the contingency mechanism mandated under the RTS.

For cases where a dedicated interface has been exempted from the contingency mechanism based on the customer interface but no longer meets the requirements for such an exemption, or cases where an ASPSP fails to offer any interface that complies with the requirements of PSD2 and the RTS, the Commission has introduced a provision to ensure business continuity in the payments market. In such a situation, competent authorities shall guarantee that PISPs and AISPs are not blocked or obstructed in the provision of their services.

**COMMISSION DELEGATED REGULATION (EU) No .../..**

**of XXX**

**supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication**

(Text with EEA relevance)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, and in particular the second subparagraph of Article 98(4) thereof<sup>1</sup>,

Whereas:

- (1) Payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. The authentication procedure should include, in general, transaction monitoring mechanisms to detect attempts to use a payment service user's personalised security credentials that were lost, stolen, or misappropriated and should also ensure that the payment service user is the legitimate user and therefore is giving consent for the transfer of funds and access to its account information through a normal use of the personalised security credentials. Furthermore, it is necessary to specify the requirements of the strong customer authentication that should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse, by requiring the generation of an authentication code which should be resistant against the risk of being forged in its entirety or by disclosure of any of the elements upon which the code was generated.
- (2) As fraud methods are constantly changing, the requirements of strong customer authentication should allow for innovation in the technical solutions addressing the emergence of new threats to the security of electronic payments. To ensure that the requirements to be laid down are effectively implemented on a continuous basis, it is also appropriate to require that the security measures for the application of strong customer authentication and its exemptions, the measures to protect confidentiality and integrity of the personalised security credentials, and the measures establishing common and secure open standards of communication are documented, periodically tested, evaluated and audited by auditors with expertise in IT security and payments and operationally independent. In order to allow competent authorities to monitor the

---

<sup>1</sup> OJ L 337, 23.12.2015 p. 35.

quality of the review of these measures, such reviews should be made available to them upon their request.

- (3) As electronic remote payment transactions are subject to a higher risk of fraud, it is necessary to introduce additional requirements for the strong customer authentication of such transactions, ensuring that the elements dynamically link the transaction to an amount and a payee specified by the payer when initiating the transaction.
- (4) Dynamic linking is possible through the generation of authentication codes which is subject to a set of strict security requirements. To remain technologically neutral a specific technology for the implementation of authentication codes should not be required. Therefore authentication codes should be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.
- (5) It is necessary to lay down specific requirements for the situation where the final amount is not known at the moment the payer initiates an electronic remote payment transaction, in order to ensure that the strong customer authentication is specific to the maximum amount that the payer has given consent for as referred to in Directive (EU) 2015/2366.
- (6) In order to ensure the application of strong customer authentication, it is also necessary to require adequate security features for the elements of strong customer authentication categorised as knowledge (something only the user knows), such as length or complexity, for the elements categorised as possession (something only the user possesses), such as algorithm specifications, key length and information entropy, and for the devices and software that read elements categorized as inherence (something the user is) such as algorithm specifications, biometric sensor and template protection features, in particular to mitigate the risk that those elements are uncovered, disclosed to and used by unauthorised parties. It is also necessary to lay down the requirements to ensure that those elements are independent, so that the breach of one does not compromise the reliability of the others, in particular when any of these elements are used through a multi-purpose device, namely a device such as a tablet or a mobile phone which can be used both for giving the instruction to make the payment and in the authentication process.
- (7) The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity.
- (8) Due to their very nature, payments made through the use of an anonymous payment instruments are not subject to the obligation of strong customer authentication. Where the anonymity of such instruments is lifted on contractual or legislative grounds, payments are subject to the security requirements that follow from Directive (EU) 2015/2366 and this Regulatory Technical Standard.
- (9) In accordance with Directive (EU) 2015/2366, exemptions to the principle of strong customer authentication have been defined based on the level of risk, amount, recurrence and the payment channel used for the execution of the payment transaction.
- (10) Actions which imply access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data, recurring payments to the same payees which have been previously set up or confirmed by the payer through the use of strong customer authentication, and payments to and from the same natural or legal person with accounts with the same payment service provider, pose a low level of risk,

thus allowing payment service providers not to apply strong customer authentication. This leaves aside that in accordance with Articles 65, 66 and 67 Directive (EU) 2015/2366, payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers should only seek and obtain the necessary and essential information from the account servicing payment service provider for the provision of a given payment service with the consent of the payment service user. Such consent can be given individually for each request of information or for each payment to be initiated or, for account information service providers, as a mandate for designated payment accounts and associated payment transactions as established in the contractual agreement with the payment service user.

- (11) Exemptions for low-value contactless payments at points of sale, which also take into account a maximum number of consecutive transactions or a certain fixed maximum value of consecutive transactions without applying strong customer authentication, allow for the development of user friendly and low risk payment services and should therefore be provided for. It is also appropriate to establish an exemption for the case of electronic payment transactions initiated at unattended terminals where the use of strong customer authentication may not always be easy to apply due to operational reasons (e.g. to avoid queues and potential accidents at toll gates or for other safety or security risks).
- (12) Similar to the exemption for low value contactless payments at the point of sale, a proper balance needs to be struck between the interest in enhanced security in remote payments and the needs of user-friendliness and accessibility of payments in the area of e-commerce. In line with those principles, thresholds below which no strong customer authentication needs to be applied should be set in a prudent manner, to cover only online purchases of low value. The thresholds for online purchases should be set more prudently, considering that the fact that the person is not physically present when making the purchase is posing a slightly higher security risk.
- (13) The requirements of strong customer authentication apply to payments initiated by the payer, regardless of whether the payer is a natural person or a legal entity. Many corporate payments are initiated through dedicated processes or protocols which guarantee the high levels of payment security that Directive (EU) 2015/2366 aims to achieve through strong customer authentication. Where the competent authorities establish that those payment processes and protocols that are only made available to payers who are not consumers achieve the objectives of Directive (EU) 2015/2366 in terms of security, payment service providers may, in relation to those processes or protocols, be exempted from the strong customer authentication requirements.
- (14) In the case of real-time transaction risk analysis that categorise a payment transaction as low risk, it is also appropriate to introduce an exemption for the payment service provider that intends not to apply strong customer authentication through the adoption of effective and risk-based requirements which ensure the safety of the payment service user's funds and personal data. Those risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioural pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments. Where, on the basis of the real-time transaction risk analysis, a payment cannot be qualified as posing a low level of risk, the payment service provider should revert to strong customer authentication. The maximum value of such risk based exemption should be set in a manner ensuring a

very low corresponding fraud rate, also by comparison to the fraud rates of all the payment transactions of the payment service provider, including those authenticated through strong customer authentication, within a certain period of time and on a rolling basis.

- (15) For the purpose of ensuring an effective enforcement, payment service providers, that wish to benefit from the exemptions from strong customer authentication should regularly monitor and make available to competent authorities and to the European Banking Authority (EBA), upon their request, for each payment transaction type, the value of fraudulent or unauthorised payment transactions and the observed fraud rates for all their payment transactions, whether authenticated through strong customer authentication or executed under a relevant exemption.
- (16) The collection of this new historical evidence on the fraud rates of electronic payment transactions will also contribute to an effective review by the EBA of the thresholds for an exemption to strong customer authentication based on a real-time transaction risk analysis. The EBA should review and submit draft updates to the Commission of these regulatory technical standards, where appropriate, by submitting new draft thresholds and corresponding fraud rates with the aim of enhancing the security of remote electronic payments, in accordance with Article 98(5) of Directive (EU) 2015/2366 and with Article 10 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council<sup>2</sup>.
- (17) Payment service providers that make use of any of the exemptions to be provided for should be allowed at any time to choose to apply strong customer authentication to the actions and to the payment transactions referred to in those provisions.
- (18) The measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, should limit the risks relating to fraud through unauthorised or fraudulent use of payment instruments and unauthorised access to payment accounts. To this end it is necessary to introduce requirements on the secure creation and delivery of the personalised security credentials and their association with the payment service user, and to provide conditions for the renewal and deactivation of those credentials.
- (19) In order to ensure effective and secure communication between the relevant actors in the context of account information services, payment initiation services and confirmation on the availability of funds, it is necessary to specify the requirements of common and secure open standards of communication to be met by all relevant payment service providers. Directive (EU) 2015/2366 provides for the access and use of payment account information by account information service providers. This regulation therefore does not change the rules of access to accounts other than payment accounts.
- (20) Each account servicing payment service provider with payment accounts that are accessible online should offer at least one access interface enabling secure communication with account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. The interface should enable the account information service providers, payment initiation

---

<sup>2</sup> Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC (OJ L 331, 15.12.2010, p. 12).



service providers and payment service providers issuing card-based payment instruments to identify themselves to the account servicing payment service provider. It should also allow account information service providers and payment initiation service providers to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user. To ensure technology and business-model neutrality, the account servicing payment service providers should be free to decide whether to offer an interface that is dedicated to the communication with account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments, or to allow, for that communication, the use of the interface for the identification and communication with the account servicing payment service providers' payment service users.

- (21) In order to allow account information service providers, payment initiation service providers, and payment service providers issuing card-based payment instruments to develop their technical solutions, the technical specification of the interface should be adequately documented and made publicly available. Moreover, the account servicing payment service provider should offer a facility enabling the payment service providers to test the technical solutions at least six months prior to the application date of these regulatory standards or, if the launch takes place after the application date of these standards, prior to the date on which the interface will be launched to the market. To ensure the interoperability of different technological communication solutions, the interface should use standards of communication which are developed by international or European standardisation organisations.
- (22) The quality of the services provided by account information service providers and payment initiation service providers will be dependent on the proper functioning of the interfaces put in place or adapted by account servicing payment service providers. It is therefore important that in case of non-compliance of such interfaces with the provisions included in these standards, measures are taken to guarantee business continuity for the benefit of the users of those services. It is the responsibility of national competent authorities to ensure that account information service providers and payment initiation service providers are not blocked or obstructed in the provision of their services.
- (23) Where access to payment accounts is offered by means of a dedicated interface, in order to ensure the right of payment service users to make use of payment initiation service providers and of services enabling access to account information, as provided for in Directive (EU) 2015/2366, it is necessary to require that dedicated interfaces have the same level of availability and performance as the interface available to the payment service user. Account servicing payment service providers should also define transparent key performance indicators and service level targets for the availability and performance of dedicated interfaces that are at least as stringent as those for the interface used for their payment service users. Those interfaces should be tested by the payment service providers who will use them, and should be stress-tested and monitored by competent authorities.
- (24) To ensure that payment service providers who rely on the dedicated interface can continue to provide their services in case of problems of availability or inadequate performance, it is necessary to provide, subject to strict conditions, a fallback mechanism that will allow such providers to use the interface that the account servicing payment service provider maintains for the identification of, and communication with, its own payment service users. Certain account servicing payment service providers will be exempted from having to provide such a fallback

mechanism through their customer facing interfaces where their competent authorities establish that the dedicated interfaces comply with specific conditions that ensure unhampered competition. In the event that the exempted dedicated interfaces fail to comply with the required conditions, the granted exemptions shall be revoked by the relevant competent authorities.

- (25) In order to allow competent authorities to effectively supervise and monitor the implementation and management of the communication interfaces, the account servicing payment service providers should make a summary of the relevant documentation available on their website, and provide, upon request, the competent authorities with documentation of the solutions in case of emergencies. The account servicing payment service providers should also make publicly available the statistics on the availability and performance of that interface.
- (26) In order to safeguard the confidentiality and the integrity of data, it is necessary to ensure the security of communication sessions between account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments. It is in particular necessary to require that secure encryption is applied between account information service providers, payment initiation service providers, payment service providers issuing card-based payment instruments and account servicing payment service providers when exchanging data.
- (27) To improve user confidence and ensure strong customer authentication, the use of electronic identification means and trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council<sup>3</sup> should be taken into account, in particular with regard to notified electronic identification schemes
- (28) In order to ensure aligned application dates, this Regulation should be applicable from the same date as of which Member States have to ensure application of the security measures referred to in Articles 65, 66, 67 and 97 of Directive 2015/2366.
- (29) This Regulation is based on the draft regulatory technical standards submitted by the European Banking Authority (EBA) to the Commission.
- (30) EBA has conducted open and transparent public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the opinion of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010.

---

<sup>3</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 53).

HAS ADOPTED THIS REGULATION:

## **CHAPTER I GENERAL PROVISIONS**

### *Article 1 Subject matter*

This Regulation establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to do the following:

- (a) apply the procedure of strong customer authentication in accordance with Article 97 of Directive (EU) 2015/2366;
- (b) exempt the application of the security requirements of strong customer authentication, subject to specified and limited conditions based on the level of risk, the amount and the recurrence of the payment transaction and of the payment channel used for its execution;
- (c) protect the confidentiality and the integrity of the payment service user's personalised security credentials;
- (d) establish common and secure open standards for the communication between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers in relation to the provision and use of payment services in application of Title IV of Directive (EU) 2015/2366.

### *Article 2 General authentication requirements*

1. Payment service providers shall have transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions for the purpose of the implementation of the security measures referred to in points (a) and (b) of Article 1.

Those mechanisms shall be based on the analysis of payment transactions taking into account elements which are typical of the payment service user in the circumstances of a normal use of the personalised security credentials.

2. Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:
  - (a) lists of compromised or stolen authentication elements;
  - (b) the amount of each payment transaction;
  - (c) known fraud scenarios in the provision of payment services;
  - (d) signs of malware infection in any sessions of the authentication procedure;
  - (e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

*Article 3*  
*Review of the security measures*

1. The implementation of the security measures referred to in Article 1 shall be documented, periodically tested, evaluated and audited in accordance with the applicable legal framework of the payment service provider by auditors with expertise in IT security and payments and operationally independent within or from the payment service provider.
2. The period between the audits referred to in paragraph 1 shall be determined taking into account the relevant accounting and statutory audit framework applicable to the payment service provider.

However, payment service providers that make use of the exemption referred to in Article 18 shall be subject to an audit of the methodology, the model and the reported fraud rates at a minimum on a yearly basis. The auditor performing this audit shall have expertise in IT security and payments and be operationally independent within or from the payment service provider. During the first year of making use of the exemption under Article 18 and at least every three years thereafter, or more frequently at the competent authority's request, this audit shall be carried out by an independent and qualified external auditor.

3. This audit shall present an evaluation and report on the compliance of the payment service provider's security measures with the requirements set out in this Regulation.  
The entire report shall be made available to competent authorities upon their request.

## **CHAPTER II**

# **SECURITY MEASURES FOR THE APPLICATION OF STRONG CUSTOMER AUTHENTICATION**

### *Article 4* *Authentication code*

1. Where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.

The authentication code shall be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

2. For the purpose of paragraph 1, payment service providers shall adopt security measures ensuring that each of the following requirements is met:

- (a) no information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code;
- (b) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;
- (c) the authentication code cannot be forged.

3. Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures:

- (a) where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, it shall not be possible to identify which of the elements referred to in that paragraph was incorrect;
- (b) the number of failed authentication attempts that can take place consecutively, after which the actions referred to in Article 97(1) of Directive (EU) 2015/2366 shall be temporarily or permanently blocked, shall not exceed five within a given period of time;
- (c) the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter V;
- (d) the maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed five minutes.

4. Where the block referred to in paragraph 3(b) is temporary, the duration of that block and the number of retries shall be established based on the characteristics of the service provided to the payer and all the relevant risks involved, taking into account, at a minimum, the factors referred to in Article 2(2).

The payer shall be alerted before the block is made permanent.

Where the block has been made permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments.

*Article 5*  
*Dynamic linking*

1. Where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366, in addition to the requirements of Article 4 of this Regulation, they shall also adopt security measures that meet each of the following requirements:
  - (a) the payer is made aware of the amount of the payment transaction and of the payee;
  - (b) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;
  - (c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;
  - (d) any change to the amount or the payee results in the invalidation of the authentication code generated.
2. For the purpose of paragraph 1, payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:
  - (a) the amount of the transaction and the payee throughout all of the phases of the authentication;
  - (b) the information displayed to the payer throughout all of the phases of the authentication including the generation, transmission and use of the authentication code.
3. For the purpose of paragraph 1(b) and where payment service providers apply strong customer authentication in accordance with Article 97(2) of Directive (EU) 2015/2366 the following requirements for the authentication code shall apply:
  - (a) in relation to a card-based payment transaction for which the payer has given consent to the exact amount of the funds to be blocked pursuant to Article 75(1) of that Directive, the authentication code shall be specific to the amount that the payer has given consent to be blocked and agreed to by the payer when initiating the transaction;
  - (b) in relation to payment transactions for which the payer has given consent to execute a batch of remote electronic payment transactions to one or several payees, the authentication code shall be specific to the total amount of the batch of payment transactions and to the specified payees.

*Article 6*  
*Requirements of the elements categorised as knowledge*

1. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties.

2. The use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.

#### *Article 7*

##### *Requirements of the elements categorised as possession*

1. Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer authentication categorised as possession are used by unauthorised parties.
2. The use by the payer of those elements shall be subject to measures designed to prevent replication of the elements.

#### *Article 8*

##### *Requirements of devices and software linked to elements categorised as inherence*

1. Payment service providers shall adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a minimum, the payment service providers shall ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer.
2. The use by the payer of those elements shall be subject to measures ensuring that those devices and the software guarantee resistance against unauthorised use of the elements through access to the devices and the software.

#### *Article 9*

##### *Independence of the elements*

1. Payment service providers shall ensure that the use of the elements of strong customer authentication referred to in Articles 6, 7 and 8 is subject to measures which ensure that, in terms of technology, algorithms and parameters, the breach of one of the elements does not compromise the reliability of the other elements.
2. Payment service providers shall adopt security measures, where any of the elements of strong customer authentication or the authentication code itself is used through a multi-purpose device, to mitigate the risk which would result from that multi-purpose device being compromised.
3. For the purposes of paragraph 2, the mitigating measures shall include each of the following:
  - (a) the use of separated secure execution environments through the software installed inside the multi-purpose device;
  - (b) mechanisms to ensure that the software or device has not been altered by the payer or by a third party;
  - (c) where alterations have taken place, mechanisms to mitigate the consequences thereof.

## **CHAPTER III**

### **EXEMPTIONS FROM STRONG CUSTOMER AUTHENTICATION**

#### *Article 10*

##### *Payment account information*

1. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2 and to paragraph 2 of this Article and, where a payment service user is limited to accessing either or both of the following items online without disclosure of sensitive payment data:
  - (a) the balance of one or more designated payment accounts;
  - (b) the payment transactions executed in the last 90 days through one or more designated payment accounts.
2. For the purpose of paragraph 1, payment service providers shall not be exempted from the application of strong customer authentication where either of the following condition is met:
  - (a) the payment service user is accessing online the information specified in paragraph 1 for the first time;
  - (b) more than 90 days have elapsed since the last time the payment service user accessed online the information specified in paragraph 1(b) and strong customer authentication was applied.

#### *Article 11*

##### *Contactless payments at point of sale*

Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where the payer initiates a contactless electronic payment transaction provided that the following conditions are met:

- (a) the individual amount of the contactless electronic payment transaction does not exceed EUR 50; and
- (b) the cumulative amount of previous contactless electronic payment transactions initiated by means of a payment instrument with a contactless functionality from the date of the last application of strong customer authentication does not exceed EUR 150; or
- (c) the number of consecutive contactless electronic payment transactions initiated via the payment instrument offering a contactless functionality since the last application of strong customer authentication does not exceed five.

#### *Article 12*

##### *Unattended terminals for transport fares and parking fees*

Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.



*Article 13*  
*Trusted beneficiaries*

1. Payment service providers shall apply strong customer authentication where a payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider.
2. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

*Article 14*  
*Recurring transactions*

1. Payment service providers shall apply strong customer authentication when a payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee.
2. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions referred to in paragraph 1.

*Article 15*  
*Credit transfers between accounts held by the same natural or legal person*

Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where the payer initiates a credit transfer in circumstances where the payer and the payee are the same natural or legal person and both payment accounts are held by the same account servicing payment service provider.

*Article 16*  
*Low-value transactions*

Payment service providers shall be allowed not to apply strong customer authentication, where the payer initiates a remote electronic payment transaction provided that the following conditions are met:

- (a) the amount of the remote electronic payment transaction does not exceed EUR 30; and
- (b) the cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed EUR 100; or
- (c) the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed 5 consecutive individual remote electronic payment transactions.

*Article 17*  
*Secure corporate payment processes and protocols*

Payment service providers shall be allowed not to apply strong customer authentication, in respect of legal persons initiating electronic payment transactions through the use of dedicated payment processes or protocols that are only made available to payers who are not consumers, where the competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those provided for by Directive 2015/2366.

*Article 18*  
*Transaction risk analysis*

1. Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.
2. An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:
  - (a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Annex for ‘remote electronic card-based payments’ and ‘remote electronic credit transfers’ respectively;
  - (b) the amount of the transaction does not exceed the relevant Exemption Threshold Value (‘ETV’) specified in the table set out in the Annex;
  - (c) payment service providers as a result of performing a real time risk analysis have not identified any of the following:
    - (i) abnormal spending or behavioural pattern of the payer;
    - (ii) unusual information about the payer’s device/software access ;
    - (iii) malware infection in any session of the authentication procedure;
    - (iv) known fraud scenario in the provision of payment services;
    - (v) abnormal location of the payer;
    - (vi) high risk location of the payee.
3. Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:
  - (a) the previous spending patterns of the individual payment service user;
  - (b) the payment transaction history of each of the payment service provider’s payment service users;
  - (c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;
  - (d) the identification of abnormal payment patterns of the payment service user in relation to the user’s payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

*Article 19*  
*Calculation of fraud rates*

1. For each type of transaction referred to in the table set out in the Annex, the payment service provider shall ensure that the overall fraud rates covering both payment transactions authenticated through strong customer authentication and those executed under any of the exemptions referred to in Articles 13 to 18 are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction indicated in the table set out in the Annex.

The overall fraud rate for each type of transaction shall be calculated as the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of transactions, whether authenticated with the application of strong customer authentication or executed under any exemption referred to in Articles 13 to 18 on a rolling quarterly basis (90 days).

2. The calculation of the fraud rates and resulting figures shall be assessed by the audit review referred to in Article 3(2), which shall ensure that they are complete and accurate.
3. The methodology and any model, used by the payment service provider to calculate the fraud rates, as well as the fraud rates themselves, shall be adequately documented and made fully available to competent authorities and to EBA, with prior notification to the relevant competent authority(ies), upon their request.

*Article 20*  
*Cessation of exemptions based on transaction risk analysis*

1. Payment service providers that make use of the exemption referred to in Article 18 shall immediately report to the competent authorities where one of their monitored fraud rates, for any type of payment transactions indicated in the table set out in the Annex, exceeds the applicable reference fraud rate and shall provide to the competent authorities a description of the measures that they intend to adopt to restore compliance of their monitored fraud rate with the applicable reference fraud rates.
2. Payment service providers shall immediately cease to make use of the exemption referred to in Article 18 for any type of payment transactions indicated in the table set out in the Annex in the specific exemption threshold range where their monitored fraud rate exceeds for two consecutive quarters the reference fraud rate applicable for that payment instrument or type of payment transaction in that exemption threshold range.
3. Following the cessation of the exemption referred to in Article 18 in accordance with paragraph 2 of this Article, payment service providers shall not use that exemption again, until their calculated fraud rate equals to, or is below, the reference fraud rates applicable for that type of payment transaction in that exemption threshold range for one quarter.

4. Where payment service providers intend to make use again of the exemption referred to in Article 18, they shall notify the competent authorities in a reasonable timeframe and shall before making use again of the exemption, provide evidence of the restoration of compliance of their monitored fraud rate with the applicable reference fraud rate for that exemption threshold range in accordance with paragraph 3 of this Article.

*Article 21*  
*Monitoring*

1. In order to make use of the exemptions set out in Articles 10 to 18, payment service providers shall record and monitor the following data for each type of payment transactions, with a breakdown for both remote and non-remote payment transactions, at least on a quarterly basis:
  - (a) the total value of unauthorised or fraudulent payment transactions in accordance with Article 64(2) of Directive (EU) 2015/2366, the total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions;
  - (b) the average transaction value, including a breakdown of payment transactions initiated through strong customer authentication and under each of the exemptions;
  - (c) the number of payment transactions where each of the exemptions was applied and their percentage in respect of the total number of payment transactions.
2. Payment service providers shall make the results of the monitoring in accordance with paragraph 1 available to competent authorities and to EBA, with prior notification to the relevant competent authority(ies), upon their request.

## **CHAPTER IV**

# **CONFIDENTIALITY AND INTEGRITY OF THE PAYMENT SERVICE USERS' PERSONALISED SECURITY CREDENTIALS**

### *Article 22*

#### *General requirements*

1. Payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of the authentication.
2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:
  - (a) personalised security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication;
  - (b) personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plaintext;
  - (c) secret cryptographic material is protected from unauthorised disclosure.
3. Payment service providers shall fully document the process related to the management of cryptographic material used to encrypt or otherwise render unreadable the personalised security credentials.
4. Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter II take place in secure environments in accordance with strong and widely recognised industry standards.

### *Article 23*

#### *Creation and transmission of credentials*

Payment service providers shall ensure that the creation of personalised security credentials is performed in a secure environment.

They shall mitigate the risks of unauthorised use of the personalised security credentials and of the authentication devices and software following their loss, theft or copying before their delivery to the payer.

### *Article 24*

#### *Association with the payment service user*

1. Payment service providers shall ensure that only the payment service user is associated, in a secure manner, with the personalised security credentials, the authentication devices and the software.
2. For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:

- (a) the association of the payment service user's identity with personalised security credentials, authentication devices and software is carried out in secure environments under the payment service provider's responsibility comprising at least the payment service provider's premises, the internet environment provided by the payment service provider or other similar secure websites used by the payment service provider and its automated teller machine services, and taking into account risks associated with devices and underlying components used during the association process that are not under the responsibility of the payment service provider;
- (b) the association by means of a remote channel of the payment service user's identity with the personalised security credentials and with authentication devices or software is performed using strong customer authentication.

#### *Article 25*

##### *Delivery of credentials, authentication devices and software*

1. Payment service providers shall ensure that the delivery of personalised security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorised use due to their loss, theft or copying.
2. For the purpose of paragraph 1, payment service providers shall at least apply each of the following measures:
  - (a) effective and secure delivery mechanisms ensuring that the personalised security credentials, authentication devices and software are delivered to the legitimate payment service user;
  - (b) mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user by means of the internet;
  - (c) arrangements ensuring that, where the delivery of personalised security credentials is executed outside the premises of the payment service provider or through a remote channel:
    - (i) no unauthorised party can obtain more than one feature of the personalised security credentials, the authentication devices or software when delivered through the same channel;
    - (ii) the delivered personalised security credentials, authentication devices or software require activation before usage;
  - (d) arrangements ensuring that, in cases where the personalised security credentials, the authentication devices or software have to be activated before their first use, the activation shall take place in a secure environment in accordance with the association procedures referred to in Article 24.

#### *Article 26*

##### *Renewal of personalised security credentials*

Payment service providers shall ensure that the renewal or re-activation of personalised security credentials adhere to the procedures for the creation, association and delivery of the credentials and of the authentication devices in accordance with Articles 23, 24 and 25.

*Article 27*  
*Destruction, deactivation and revocation*

Payment service providers shall ensure that they have effective processes in place to apply each of the following security measures:

- (a) the secure destruction, deactivation or revocation of the personalised security credentials, authentication devices and software;
- (b) where the payment service provider distributes reusable authentication devices and software, the secure re-use of a device or software is established, documented and implemented before making it available to another payment services user;
- (c) the deactivation or revocation of information related to personalised security credentials stored in the payment service provider's systems and databases and, where relevant, in public repositories.

**CHAPTER V**  
**COMMON AND SECURE OPEN STANDARDS OF**  
**COMMUNICATION**

**SECTION 1**  
**GENERAL REQUIREMENTS FOR COMMUNICATION**

*Article 28*  
*Requirements for identification*

1. Payment service providers shall ensure secure identification when communicating between the payer's device and the payee's acceptance devices for electronic payments, including but not limited to payment terminals.
2. Payment service providers shall ensure that the risks of misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.

*Article 29*  
*Traceability*

1. Payment service providers shall have processes in place which ensure that all payment transactions and other interactions with the payment services user, with other payment service providers and with other entities, including merchants, in the context of the provision of the payment service are traceable, ensuring knowledge ex-post of all events relevant to the electronic transaction in all the various stages.
2. For the purpose of paragraph 1, payment service providers shall ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies on each of the following:
  - (a) a unique identifier of the session;
  - (b) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data;

- (c) timestamps which shall be based on a unified time-reference system and which shall be synchronised according to an official time signal.

## **SECTION 2**

### **SPECIFIC REQUIREMENTS FOR THE COMMON AND SECURE OPEN STANDARDS OF COMMUNICATION**

#### *Article 30*

##### *General obligations for access interfaces*

1. Account servicing payment service providers that offer to a payer a payment account that is accessible online shall have in place at least one interface which meets each of the following requirements:
  - (a) account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments are able to identify themselves towards the account servicing payment service provider;
  - (b) account information service providers are able to communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions;
  - (c) payment initiation service providers are able to communicate securely to initiate a payment order from the payer's payment account and receive all information on the initiation of the payment transaction and all information accessible to the account servicing payment service providers regarding the execution of the payment transaction.
  
2. For the purposes of authentication of the payment service user, the interface referred to in paragraph 1 shall allow account information service providers and payment initiation service providers to rely on all the authentication procedures provided by the account servicing payment service provider to the payment service user.

The interface shall at least meet all of the following requirements:

  - (a) a payment initiation service provider or an account information service provider shall be able to instruct the account servicing payment service provider to start the authentication based on the consent of the payment service user;
  - (b) communication sessions between the account servicing payment service provider, the account information service provider, the payment initiation service provider and any payment service user concerned shall be established and maintained throughout the authentication;
  - (c) the integrity and confidentiality of the personalised security credentials and of authentication codes transmitted by or through the payment initiation service provider or the account information service provider shall be ensured.
  
3. Account servicing payment service providers shall ensure that their interfaces follow standards of communication which are issued by international or European standardisation organisations.

Account servicing payment service providers shall also ensure that the technical specification of any of the interfaces is documented specifying a set of routines, protocols, and tools needed by payment initiation service providers, account information service providers and payment service providers issuing card-based



payment instruments for allowing their software and applications to interoperate with the systems of the account servicing payment service providers.

Account servicing payment service providers shall at a minimum, and no less than six months before the application date referred to in Article 38(2), or before the target date for the market launch of the access interface when the launch takes place after the date referred to in Article 38(2), make the documentation available, at no charge, upon request by authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments or payment service providers that have applied to their competent authorities for the relevant authorisation, and shall make a summary of the documentation publicly available on their website.

4. In addition to paragraph 3, account servicing payment service providers shall ensure that, except for emergency situations, any change to the technical specification of their interface is made available to authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, or payment service providers that have applied to their competent authorities for the relevant authorisation, in advance as soon as possible and not less than 3 months before the change is implemented.

Payment service providers shall document emergency situations where changes were implemented and make the documentation available to competent authorities on request.

5. Account servicing payment service providers shall make available a testing facility, including support, for connection and functional testing to enable authorised payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users. This testing facility should be made available no later than six months before the application date referred to in Article 38(2) or before the target date for the market launch of the access interface when the launch takes place after the date referred to in Article 38(2).

However, no sensitive information shall be shared through the testing facility.

6. Competent authorities shall ensure that account servicing payment service providers comply at all times with the obligations included in these standards in relation to the interface(s) that they put in place. In the event that an account servicing payment services provider fails to comply with the requirements for interfaces laid down in these standards, competent authorities shall ensure that the provision of payment initiation services and account information services is not prevented or disrupted to the extent that the respective providers of such services comply with the conditions defined under Article 33(5).

### *Article 31* *Access interface options*

Account servicing payment service providers shall establish the interface(s) referred to in Article 30 by means of a dedicated interface or by allowing the use by the payment service providers referred to in Article 30(1) of the interfaces used for authentication and communication with the account servicing payment service provider's payment services users.

*Article 32*  
*Obligations for a dedicated interface*

1. Subject to compliance with Article 30 and 31, account servicing payment service providers that have put in place a dedicated interface shall ensure that the dedicated interface offers at all times the same level of availability and performance, including support, as the interfaces made available to the payment service user for directly accessing its payment account online.
2. Account servicing payment service providers that have put in place a dedicated interface shall define transparent key performance indicators and service level targets, at least as stringent as those set for the interface used by their payment service users both in terms of availability and of data provided in accordance with Article 36. Those interfaces, indicators and targets shall be monitored by the competent authorities and stress-tested.
3. Account servicing payment service providers that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services. Such obstacles, may include, among others, preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing payment service provider's authentication or other functions, requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive 2015/2366, or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.
4. For the purpose of paragraphs 1 and 2, account servicing payment service providers shall monitor the availability and performance of the dedicated interface. Account servicing payment service providers shall publish on their website quarterly statistics on the availability and performance of the dedicated interface and of the interface used by its payment service users.

*Article 33*  
*Contingency measures for a dedicated interface*

1. Account servicing payment service providers shall include, in the design of the dedicated interface, a strategy and plans for contingency measures for the event that the interface does not perform in compliance with Article 32, that there is unplanned unavailability of the interface and that there is a systems breakdown. Unplanned unavailability or a systems breakdown may be presumed to have arisen when five consecutive requests for access to information for the provision of payment initiation services or account information services are not replied to within 30 seconds.
2. Contingency measures shall include communication plans to inform payment service providers making use of the dedicated interface of measures to restore the system and a description of the immediately available alternative options payment service providers may have during this time.
3. Both the account servicing payment service provider and the payment service providers referred to in Article 30(1) shall report problems with dedicated interfaces as described in paragraph 1 to their respective competent national authorities without delay.

4. As part of a contingency mechanism, payment service providers referred to in Article 30(1) shall be allowed to make use of the interfaces made available to the payment service users for the authentication and communication with their account servicing payment service provider, until the dedicated interface is restored to the level of availability and performance provided for in Article 32.
5. For this purpose, account servicing payment service providers shall ensure that the payment service providers referred to in Article 30(1) can be identified and can rely on the authentication procedures provided by the account servicing payment service provider to the payment service user. Where the payment service providers referred to in Article 30(1) make use of the interface referred to in paragraph 4 they shall:
  - (a) take the necessary measures to ensure that they do not access, store or process data for purposes other than for the provision of the service as requested by the payment service user;
  - (b) continue to comply with the obligations following from Article 66(3) and Article 67(2) of Directive (EU) 2015/2366 respectively;
  - (c) 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 their competent national authority;
  - (d) duly justify to their competent national authority, upon request and without undue delay, the use of the interface made available to the payment service users for directly accessing its payment account online;
  - (e) inform the account servicing payment service provider accordingly.
6. Competent authorities, after consulting EBA to ensure a consistent application of the following conditions, shall exempt the account servicing payment service providers that have opted for a dedicated interface from the obligation to set up the contingency mechanism described under paragraph 4 where the dedicated interface meets all of the following conditions:
  - (a) it complies with all the obligations for dedicated interfaces as set out in Article 32;
  - (b) it has been designed and tested in accordance with Article 30(5) to the satisfaction of the payment service providers referred to therein;
  - (c) it has been widely used for at least three months by payment service providers to offer account information services, payment initiation services and to provide confirmation on the availability of funds for card-based payments;
  - (d) any problem related to the dedicated interface has been resolved without undue delay.
7. Competent authorities shall revoke the exemption referred to in paragraph 6 where the conditions (a) and (d) are not met by the account servicing payment service providers for more than two consecutive calendar weeks. Competent authorities shall inform EBA of this revocation and shall ensure that the account servicing payment service provider establishes, within the shortest possible time and at the latest within two months, the contingency mechanism referred to in paragraph 4.

*Article 34*  
*Certificates*

1. For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation.
2. For the purpose of this Regulation, the registration number as referred to in the official records in accordance with Annex III (c) or Annex IV (c) to Regulation (EU) No 910/2014 shall be the authorisation number of the payment service provider issuing card-based payment instruments, the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available in the public register of the home Member State pursuant to Article 14 of Directive (EU) 2015/2366 or resulting from the notifications of every authorisation granted under Article 8 of Directive 2013/36/EU of the European Parliament and of the Council<sup>4</sup> in accordance with Article 20 of that Directive.
3. For the purposes of this Regulation, qualified certificates for electronic seals or for website authentication referred to in paragraph 1 shall include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following:
  - (a) the role of the payment service provider, which maybe one or more of the following:
    - (i) account servicing;
    - (ii) payment initiation;
    - (iii) account information;
    - (iv) issuing of card-based payment instruments;
  - (b) the name of the competent authorities where the payment service provider is registered.
4. The attributes referred to in paragraph 3 shall not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

*Article 35*  
*Security of communication session*

1. Account servicing payment service providers, payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall ensure that, when exchanging data by means of the internet, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

---

<sup>4</sup> Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

2. Payment service providers issuing card-based payment instruments, account information service providers and payment initiation service providers shall keep the access sessions offered by account servicing payment service providers as short as possible and they shall actively terminate any such session as soon as the requested action has been completed.
3. When maintaining parallel network sessions with the account servicing payment service provider, account information service providers and payment initiation service providers shall ensure that those sessions are securely linked to relevant sessions established with the payment service user(s) in order to prevent the possibility that any message or information communicated between them could be misrouted.
4. Account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments with the account servicing payment service provider shall contain unambiguous references to each of the following items:
  - (a) the payment service user or users and the corresponding communication session in order to distinguish several requests from the same payment service user or users;
  - (b) for payment initiation services, the uniquely identified payment transaction initiated;
  - (c) for confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of the card-based payment transaction.
5. Account servicing payment service providers, account information service providers, payment initiation service providers and payment service providers issuing card-based payment instruments shall ensure that where they communicate personalised security credentials and authentication codes, these are not readable, directly or indirectly, by any staff at any time.

In case of loss of confidentiality of personalised security credentials under their sphere of competence, those providers shall inform without undue delay the payment services user associated with them and the issuer of the personalised security credentials.

#### *Article 36*

#### *Data exchanges*

1. Account servicing payment service providers shall comply with each of the following requirements:
  - (a) they shall provide account information service providers with the same information from designated payment accounts and associated payment transactions made available to the payment service user when directly requesting access to the account information, provided that this information does not include sensitive payment data;
  - (b) they shall, immediately after receipt of the payment order, provide payment initiation service providers with the same information on the initiation and execution of the payment transaction provided or made available to the payment service user when the transaction is initiated directly by the latter;

- (c) they shall, upon request, immediately provide payment service providers with a confirmation in a simple 'yes' or 'no' format, whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer.
2. In case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements, the account servicing payment service provider shall send a notification message to the payment initiation service provider or the account information service provider and the payment service provider issuing card-based payment instruments which explains the reason for the unexpected event or error.

Where the account servicing payment service provider offers a dedicated interface in accordance with Article 32, the interface shall provide for notification messages concerning unexpected events or errors to be communicated by any payment service provider that detects the event or error to the other payment service providers participating in the communication session.

3. Account information service providers shall have in place suitable and effective mechanisms that prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the user's explicit consent.
4. Payment initiation service providers shall provide account servicing payment service providers with the same information as requested from the payment service user when initiating the payment transaction directly.
5. Account information service providers shall be able to access information from designated payment accounts and associated payment transactions held by account servicing payment service providers for the purposes of performing the account information service in either of the following circumstances:
  - (a) whenever the payment service user is actively requesting such information;
  - (b) where the payment service user does not actively request such information, no more than four times in a 24 hour period, unless a higher frequency is agreed between the account information service provider and the account servicing payment service provider, with the payment service user's consent.

## **CHAPTER VI**

### **FINAL PROVISIONS**

#### *Article 37* *Review*

Without prejudice to Article 98(5) of Directive (EU) 2015/2366, EBA shall review by [*OP: please insert date corresponding to '18 months after the date of application referred to in Article 38(2)*] the fraud rates referred to in the Annex to this Regulation as well as the exemptions granted under Article 33(6) in relation to dedicated interfaces and, if appropriate, submit draft updates thereto to the Commission in accordance with Article 10 of Regulation (EU) No 1093/2010.

*Article 38*  
*Entry into force*

1. This Regulation shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.
2. This Regulation shall apply from [OP: please insert date corresponding to '18 months after entry into force date'].
3. However, paragraphs 3 and 5 of Article 30 shall apply [OP: please insert date corresponding to 12 months after entry into force date].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 27.11.2017

*For the Commission*  
*The President*  
*Jean-Claude JUNCKER*