EUROPEAN
COMMISSION

Brussels, 3.8.2022
C(2022) 5517 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 3.8.2022

amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/389 as regards the 90-day exemption for account access

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

The European Banking Authority (EBA) was mandated under Article 98(1) of Directive (EU) 2015/2366 (the Payment Services Directive or PSD2) to develop draft regulatory technical standards (RTS) on strong customer authentication and common and secure open standards of communication (SCA&CSC). The RTS had to specify a number of requirements, including for strong customer authentication (SCA) and exemptions from its application. The RTS on SCA&CSC subsequently developed by the EBA was adopted by the Commission on 27 November 2017 and published in the Official Journal of the EU as Commission Delegated Regulation (EU) 2018/389, which has applied since 14 September 2019.

In accordance with Article 98(5) of the PSD2, the EBA is required to review and, if appropriate, update the RTS on a regular basis in order, *inter alia*, to take account of innovation and technological developments. Power is delegated to the Commission to adopt the RTS in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010, as amended by Regulation (EU) 2019/2175 establishing the EBA. In accordance with Article 10(1) of Regulation (EU) No 1093/2010, the Commission must decide within 3 months of receipt of the draft standards whether to adopt them. The Commission may adopt the draft standards in part only, or with amendments, where the Union's interests so require.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

In accordance with Article 10(1) of Regulation (EU) No 1093/2010, the EBA carried out a public consultation on the draft amending RTS submitted to the Commission. A consultation paper was published on the EBA's website on 28 October 2021 and the consultation closed on 25 November 2021. The EBA requested the advice of the Banking Stakeholder Group referred to in Article 37 of Regulation (EU) No 1093/2010 on the draft amending RTS and submitted an explanation of how it took the outcome of the consultations into account when developing the final draft amending RTS it submitted to the Commission.

In accordance with Article 10(1) of Regulation (EU) No 1093/2010, the EBA also submitted its impact assessment to the Commission, including its analysis of costs and benefits, for the final draft amending RTS. The analysis is available at https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2, pages 20-24 of the final report on the draft amending RTS.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

The final draft amending RTS introduces into Commission Delegated Regulation 2018/389 a new mandatory exemption from the requirement to apply SCA. Under the exemption, account providers must not apply SCA when customers use an account information service provider to access their payment account information, if certain conditions are met that are aimed at ensuring the safety and security of the payment service user's data. This includes that data must be limited in scope, the account service payment service provider (ASPSP) has to apply SCA for the first access and periodically renew it, and the ASPSP may at any time decide to apply SCA if it has objectively justified and duly evidenced reasons for unauthorised or fraudulent access. The draft amending RTS limits in parallel the scope of application of the voluntary exemption in Article 10 of Commission Delegated Regulation (EU) 2018/389 to instances where the customer accesses the account information directly. Furthermore, the

draft amending RTS extends the timeline for the renewal of SCA from every 90 days to every 180 days where the above-mentioned exemptions apply. ASPSPs that offer both a dedicated interface and a contingency mechanism are not required to implement the SCA exemption in the contingency mechanism, provided that they do not apply the SCA exemption in their direct customer channels.

COMMISSION DELEGATED REGULATION (EU) …/...

of 3.8.2022

amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/389 as regards the 90-day exemption for account access

(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[1], and in particular Article 98(4), second subparagraph, thereof,

Whereas:

(1) Article 10 of Commission Delegated Regulation (EU) 2018/389[2] provides for an exemption from the requirement laid down in Article 97 of Directive (EU) 2015/2366 to apply strong customer authentication where a payment service user is accessing the balance and the recent transactions of a payment account without disclosure of sensitive payment data. In that case, payment service providers are allowed not to apply strong customer authentication for accessing the account information, provided that strong customer authentication was applied when the account information was accessed for the first time, and at least every 90 days after that.

(2) The use of that exemption has led to very divergent practices in the application of Delegated Regulation (EU) 2018/389, where some account servicing payment service providers request strong customer authentication every 90 days, others at shorter time intervals, and some have not applied the exemption and request strong customer authentication for every account access. That divergence has led to undesirable friction in the customer journey when using account information services and to a negative impact on the services of account information service providers.

(3) In order to ensure proper balance between the objectives of Directive (EU) 2015/2366 of enhancing security, facilitating innovation and enhancing competition in the internal market, it is necessary to further specify the application of the exemption set out in Article 10 of Delegated Regulation (EU) 2018/389, for cases where the account information is accessed through an account information service provider. Accordingly, in such a case, payment service providers should not be allowed to choose whether or not to apply strong customer authentication, and the exemption should be made

[1] OJ L 337, 23.12.2015, p. 35.

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

mandatory, subject to conditions that aim to ensure that the safety and security of the payment service users' data is being met.

(4) The exemption should be limited to access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data. The exemption should only apply where strong customer authentication was already applied by payment service providers for the first access through the respective account information service provider and should be renewed periodically.

(5) To ensure the safety and security of payment service users' data, payment service providers should, at any time, be allowed to apply strong customer authentication where they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access. This might be the case where the transaction monitoring mechanisms of the account servicing payment service provider detect an elevated risk of unauthorised or fraudulent access. In order to ensure a consistent application of the exemption, account servicing payment service providers should in such cases document and duly justify to their national competent authority, upon its request, the reasons for applying strong customer authentication.

(6) Where the payment service user directly accesses the account information, payment service providers should continue to be allowed to choose whether to apply strong customer authentication. This is because in such cases no particular issues have been observed requiring an amendment of the exemption laid down in Article 10 of Delegated Regulation (EU) 2018/389, contrary to the case of access through an account information service provider.

(7) To ensure a level playing field among all payment service providers, and in line with the objectives of Directive (EU) 2015/2366 of enabling the development of user-friendly and innovative services, it is proportionate to establish the same 180-day timeline for both the renewal of strong customer authentication for accessing the account information directly with the account servicing payment service provider and through an account information service provider. Renewing strong customer authentication at the current frequency could cause undesirable friction in the customer journey and prevent account information service providers from offering their services and users from receiving those services.

(8) Account servicing payment service providers that offer a dedicated interface and that have implemented a contingency mechanism as set out in Article 33(4) of Delegated Regulation (EU) 2018/389 should not be required to implement the new mandatory exemption in their direct customer interfaces for the purpose of the contingency mechanism, provided that they do not apply the exemption laid down in Article 10 of Delegated Regulation (EU) 2018/389 in their direct customer interfaces. It would be disproportionate to require account servicing payment service providers that offer a dedicated interface in which they have to implement the new mandatory exemption, to also implement the exemption in their direct customer interfaces for the purpose of the contingency mechanism.

(9) In order to ensure that payment service providers have sufficient time to make the necessary changes to their systems, account servicing payment service providers should make available to the payment service providers the changes made to the technical specifications of their interfaces in order to comply with this Regulation no less than 2 months before such changes are implemented.

(10) Delegated Regulation (EU) 2018/389 should therefore be amended accordingly.

(11) This Regulation is based on the draft regulatory technical standards submitted to the Commission by the European Banking Authority.

(12) The European Banking Authority has conducted open public consultations on the draft regulatory technical standards on which this Regulation is based, analysed the potential related costs and benefits and requested the advice of the Banking Stakeholder Group established in accordance with Article 37 of Regulation (EU) No 1093/2010 of the European Parliament and of the Council[3].

(13) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered formal comments on 7 June 2022.

(14) To allow for a smooth transition to the new requirements set out in this Regulation, payment service providers that have applied the exemption laid down in Article 10 of Delegated Regulation (EU) 2018/389 prior to the date of application of this Regulation should be allowed to continue applying that exemption up to 90 days from the last time strong customer authentication was applied,

HAS ADOPTED THIS REGULATION:

Article 1
Amendments to Delegated Regulation (EU) 2018/389

Delegated Regulation (EU) 2018/389 is amended as follows:

(1) Article 10 is replaced by the following:

'Article 10

Access to the payment account information directly with the account servicing payment service provider

1. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the requirements laid down in Article 2, where a payment service user is accessing its payment account online directly, provided that access is limited to one 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. By way of derogation from paragraph 1, payment service providers shall not be exempted from the application of strong customer authentication where one of the following conditions is met:

[3] 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).

(a) the payment service user is accessing online the information specified in paragraph 1 for the first time;

(b) more than 180 days have elapsed since the last time the payment service user accessed online the information specified in paragraph 1 and strong customer authentication was applied.';

(2) the following Article 10a is inserted:

'Article 10a

Access to the payment account information through an account information service provider

1. Payment service providers shall not apply strong customer authentication where a payment service user is accessing its payment account online through an account information service provider, provided that access is limited to one 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. By way of derogation from paragraph 1, payment service providers shall apply strong customer authentication where one of the following conditions is met:

(a) the payment service user is accessing online the information specified in paragraph 1 for the first time through the account information service provider;

(b) more than 180 days have elapsed since the last time the payment service user accessed online the information specified in paragraph 1 through the account information service provider and strong customer authentication was applied.

3. By way of derogation from paragraph 1, payment service providers shall be allowed to apply strong customer authentication where a payment service user is accessing its payment account online through an account information service provider and the payment service provider has objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account. In such a case, the payment service provider shall document and duly justify to its competent national authority, upon request, the reasons for applying strong customer authentication.

4. Account servicing payment service providers that offer a dedicated interface as referred to in Article 31 shall not be required to implement the exemption laid down in paragraph 1 of this Article for the purpose of the contingency mechanism referred to in Article 33(4), where they do not apply the exemption laid down in Article 10 in the direct interface used for authentication and communication with their payment service users.';

(3) in Article 30, the following paragraph 4a is inserted:

‘4a. By way of derogation from paragraph 4, account servicing payment service providers shall make available to the payment service providers referred to in this Article the changes made to the technical specifications of their interfaces in order to comply with Article 10a not less than 2 months before such changes are implemented.’.

Article 2
Transitional provisions

1. Payment service providers that applied the exemption in Article 10 of Delegated Regulation (EU) 2018/389 before … [OJ please insert a date: 7 months after the date of entry into force of this Regulation] shall be allowed to continue to apply that exemption for access requests received through an account information service provider up to the expiry of the period covered by that exemption.

2. By way of derogation from paragraph 1, whenever a new strong customer authentication is applied for access request through an account information service provider before the expiry of the period covered by the exemption referred to in paragraph 1, Article 10a as introduced by this Regulation applies.

Article 3
Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from … [OJ please insert a date: 7 months after the date of entry into force of this Regulation].

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

Done at Brussels, 3.8.2022

For the Commission
The President
Ursula VON DER LEYEN