EBA/CP/2021/32

28 October 2021

Consultation Paper

On Draft Regulatory Technical Standards

amending the Commission Delegated Regulation (EU) 2018/389 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

Contents

Responding to this consultation

The EBA invites comments on all proposals put forward in this paper and in particular on the specific questions summarised in 5.2.

Comments are most helpful if they:

- respond to the question stated;
- indicate the specific point to which a comment relates;
- contain a clear rationale;
- provide evidence to support the views expressed/ rationale proposed; and
- describe any alternative regulatory choices the EBA should consider.

Submission of responses

To submit your comments, click on the 'send your comments' button on the consultation page by 25.11.2021. Please note that comments submitted after this deadline, or submitted via other means may not be processed.

Publication of responses

Please clearly indicate in the consultation form if you wish your comments to be disclosed or to be treated as confidential. A confidential response may be requested from us in accordance with the EBA's rules on public access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the EBA's Board of Appeal and the European Ombudsman.

Data protection

The protection of individuals with regard to the processing of personal data by the EBA is based on Regulation (EU) 1725/2018 of the European Parliament and of the Council of 23 October 2018. Further information on data protection can be found under the Legal notice section of the EBA website.

Executive Summary

The revised Payment Services Directive (EU) 2015/2366 (PSD2) has introduced the requirement for payment service providers (PSPs) to apply strong customer authentication (SCA) each time a payment service user (PSU) accesses its payment account online. At the same time, the PSD2 mandated the EBA to develop regulatory technical standards (RTS) specifying, amongst others, the requirements of SCA and the exemptions to SCA, taking into account *inter alia* the at times competing objectives of PSD2, such as enhancing the security of payment services through additional authentication steps on the one hand, and of promoting user-friendly services on the other.

In particular, Article 10 of the RTS provides an exemption from the application of SCA when the customer accesses limited payment account information, provided that SCA is applied for the first access and at least every 90 days after that. When developing the RTS in 2016, the EBA introduced this exemption because, without it, the requirement set out in PSD2 would have required SCA to be applied for every single access, which would have undermined the business viability of account information services that the PSD2 has sought to promote as a new innovative service in the EU.

In line with the legal advice received at the time of developing the RTS as to how to interpret the nature of the exemptions, the EBA conceived this exemption, as well as all other exemptions to SCA in the RTS, to be of a voluntary nature, meaning that the account servicing payment service provider (ASPSP) is allowed, but not obliged to apply the exemption. The argument followed the consideration that the ASPSP is responsible under the PSD2 for performing SCA and bears the liability resulting from unauthorised or fraudulent access or transactions if it fails to protect the security of the payment service user's data. For these reasons, the RTS do not prevent ASPSPs from applying SCA even where an exemption is available that can be used.

However, with regard to the particular exemption of 90-days under Article 10 RTS, the experience gained in the first years of the application of the RTS has shown that the voluntary nature of the exemption has led to very divergent practices across the EU in its application, with some ASPSPs requesting SCA every 90-days, others at shorter time intervals, whilst others still do not apply the exemption at all and request SCA for every account access.

This has in turn led to undesirable friction for customers when using account information services, and to a negative impact on the services of account information service providers (AISPs). More specifically, the frequent application of SCA and/or the inconsistent of the exemption have been particularly detrimental for AIS use cases that rely on the AISP's possibility of accessing the account without the customer being present, as well as for AISPs that aggregate multiple accounts held by the customer with different account providers, where the customer needs to perform several SCAs, one with each account provider, in order to maintain the AISP's access to those accounts.

To address these issues, the EBA has arrived at the view that there is a need to bring further harmonisation in the application of the exemption, for the specific use case when the account information is accessed through an AISP. To that end, the EBA is proposing to make the exemption mandatory for ASPSPs for said use case, subject to certain safeguards and conditions being met that are aimed at ensuring the safety of the PSU's data, and which are: the data that can be accessed through the exemption has to be limited in scope, the ASPSP has to apply SCA for the first access and renew it periodically, and the possibility for the ASPSP to revert, at any time, to SCA if it has objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access.

For the other, separate case where customers access the data directly, the EBA is proposing to retain the exemption in Article 10 to be voluntary as is currently the case, as no specific issues have been identified in such cases. However, in order to ensure a level playing field amongst all PSPs, the EBA is also proposing to extend the 90-days timeline for the renewal of SCA to the same 180 days period for the renewal of SCA when the account data is accessed through an AISP.

The amendments proposed in this Consultation Paper are those that the EBA is legally in a position to make to address the issues identified. Other mitigations to address other issues are conceivable but would require changes to the Directive itself, which is beyond the EBA's powers to bring about.

Next steps

Given the targeted nature of the amendments proposed in this Consultation Paper and the urgency of addressing the issues at stake, in line with Article 10 of the EBA Regulation[1], the consultation period is reduced and will run from 27.10.2021 to 25.11.2021.

The amending RTS will be finalised and submitted to the Commission for endorsement following the completion of the public consultation.

[1] 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, 15.12.2020, p. 12)

Background and rationale

3.1 Background

1. The revised Payment Services Directive (EU) 2015/2366 (PSD2) requires payment service providers (PSPs) to apply strong customer authentication (SCA) each time a payment service user (PSU) 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 abuses.

2. Article 98(1) of PSD2 mandated the EBA to develop regulatory technical standards (RTS) specifying, among others, the requirements of SCA and the exemptions from the application of SCA. The PSD2 provides that, in developing the RTS, the EBA should take into account the following objectives:

    - ensuring an appropriate level of security for PSUs and PSPs, through the adoption of effective and risk-based requirements;
    - ensuring the safety of PSUs' funds and personal data;
    - securing and maintaining fair competition among all PSPs;
    - ensuring technology and business-model neutrality; and
    - allowing for the development of user-friendly, accessible and innovative means of payment.

3. Article 98(3) PSD2 also provides that the exemptions to SCA should be based on the following criteria: (a) the level of risk involved in the service provided; (b) the amount, the recurrence of the transaction, or both; and (c) the payment channel used for the execution of the transaction.

4. In fulfilment of this mandate, the EBA developed the RTS on strong customer authentication and common and secure open standards of communication (the RTS on SCA and CSC). The RTS were published in the Official Journal of the EU on 13 March 2018 as an EU Delegated Regulation and are directly applicable across the EU as of 14 September 2019.

5. The RTS contain nine exemptions to SCA, one of which (in Article 10) concerns the access to payment account information. Said exemption allows PSPs not to apply SCA where the PSU accesses the balance of the account and the recent transaction history, without disclosure of sensitive payment data (i.e, as long as no sensitive payment data is disclosed). In such case, SCA must still be applied when the account information is accessed for the first time, and at least every 90 days after that. The exemption applies both when the PSU accesses the account directly, or through an account information service provider (AISP).

6. When developing the RTS in 2016, the EBA introduced this exemption in consideration of the low level of risk involved and also because, without it, the requirement set out in PSD2 would have required SCA to be applied for every single access, which would have undermined the business viability of account information services, that the PSD2 has sought to promote as a new innovative service in the EU.

7. In line with the legal advice received at the time of developing the RTS in 2016 as to how to interpret the nature of the exemptions, the EBA conceived the exemptions to SCA, including the exemption in Article 10, to be of a voluntary nature, meaning that PSPs are allowed, but not obliged to apply the exemption. The argument followed the consideration that, in line with Articles 97(5) and 67(2)(b) of PSD2, read together with Recital 30 of the PSD2, the PSP applying SCA is the PSP that issues the personalised security credentials, namely the account servicing payment service provider (ASPSP). Accordingly, it is the ASPSP who has the obligation under PSD2 to perform SCA and who bears the liability resulting from non-authorised or fraudulent transactions or access if it fails to protect the security of the payment service user's data. For these reasons, the RTS do not restrict ASPSPs from applying SCA even where an exemption can be used.

8. However, the experience gained in the first years of the application of the RTS has shown that, with regard to this particular exemption in Article 10, the voluntary nature of the exemption has led to very divergent practices in its application, with some ASPSPs requesting SCA every 90-days, others at shorter time intervals, whilst a third group of ASPSPs have not applied the exemption at all and request SCA for every account access.

9. This has, in turn, led to undesirable friction for customers when using account information services, and to a negative impact on AISPs' services, particularly in some cases where ASPSPs have implemented a redirection or decoupled approach for SCA. More specifically, the inconsistent application of the exemption, and/or the frequent requirement to apply SCA, have had a detrimental impact on AISPs' services, due to the added friction in the customer journey caused by the authentication experience offered by ASPSPs.

10. This has been particularly the case where AISPs aggregate multiple accounts held by the customer with different account providers and where the customer has to perform several SCAs, one with each account provider and often at different points in time in order to maintain the AISP's access to the accounts. In such cases, the requirement to apply SCA may make the process of maintaining the AISP's access to those accounts too cumbersome for customers especially if the authentication experience offered by the account providers is not user-friendly.

11. Moreover, the application of SCA for each account access where ASPSPs do not apply the exemption has been particularly detrimental for AIS use cases that rely on the AISPs' possibility to access the account without the customer being present, such as certain financial management services that provide notifications to customers based on their transaction data. This is because, in such cases, the application of SCA for each account access does not allow AISPs to access the data without the customer being present.

12. Having assessed these issues, the EBA has arrived at the view that there is a need to bring further harmonisation in the application of this exemption, for the case when the access to account information is done through an AISP. To that end, the EBA is proposing to make a targeted amendment to the RTS, by making the exemption mandatory for ASPSPs, only for the specific use case when the access is done through an AISP and only if certain safeguards and conditions are met, that are aimed at ensuring the safety of the PSU's data.

13. Furthermore, in order to mitigate the impact that these issues are having on AISPs' services and to ensure a level playing field amongst all PSPs, the EBA is proposing to extend the existing 90-days timeline for the renewal of SCA in Article 10 exemption to 180-days, both where the information is accessed through an AISP or directly by the customer. The resultant amendments to the RTS that the EBA is proposing are explained in further detail below.

14. The approach proposed in this Consultation Paper (CP), and explained in the rationale section below, is specific to this particular exemption, and not to other exemptions to SCA in the RTS, given the particularity of this exemption and the issues that arose in its application.

3.2 Rationale

15. This chapter elaborates on the policy options that have been considered by the EBA in order to address the issues at stake, and the reasoning for the decisions the EBA has taken during the development of the draft amending RTS that is being proposed in this CP. In particular, the first part of this chapter explains two of the approaches that had initially been considered but eventually discarded by the EBA, whilst the second part of the chapter elaborates on the reasoning of the policy option eventually chosen by the EBA and proposed in this CP.

3.2.1 Approaches considered, but discarded

16. Since the application date of the RTS on 14 September 2019, a number of market participants have approached the EBA arguing that, in order to address the issues at stake, the EBA should either:

- require ASPSPs to delegate SCA to AISPs; or
- require SCA only once, when the customer first connects the account to the AISP and remove the requirement to apply SCA for subsequent accesses through the AISP.

17. The arguments raised by said market participants, and the EBA's assessment, are explained below.

Mandatory delegation of SCA

18. Some market participants have argued that, in order to address the issues at hand, the EBA should require ASPSPs to delegate SCA to AISPs in order for the latter to conduct SCA on the ASPSP's behalf. In these market participants' view, this would allow AISPs to offer customers a more

seamless experience when using account information services and avoid the negative impact that ASPSPs' authentication procedures are having on AISPs' services.

19. In this respect, as previously clarified in paragraphs 37-38 of the EBA Opinion on the implementation of the RTS on SCA&CSC (EBA-Op-2018-04)[2], and in paragraph 32 of the EBA Opinion on obstacles (EBA/OP/2020/10)[3], the EBA is of the view that ASPSPs cannot be obliged to delegate SCA to AISPs in order for the latter to conduct SCA on the ASPSP's behalf. This is because, in line with Articles 97(5) and 67(2)(b) of PSD2, the PSP applying SCA is the PSP that issues the personalised security credentials (namely the ASPSP). Accordingly, it is the ASPSP that has the obligation and responsibility under PSD2 to perform SCA. Whilst the ASPSP may choose to contract with AISPs in order for the latter to conduct SCA on the ASPSP's behalf, ASPSPs cannot be obliged to do so.

20. Therefore, a mandatory delegation of SCA is not possible under the PSD2, can also not be brought about by amending the RTS on SCA&CSC, and would require a change of the PSD2, which is not within the EBA's powers to bring about.

Requiring SCA only once, when the customer first connects their account to an AISP, and removing the requirement to apply SCA for subsequent accesses through the AISP

21. Some market participants have argued that, in order to address the issues at stake, SCA should be required only once, when the customer first connects their account to the AISP and not for subsequent accesses to the account information through the AISP. Said market participants have argued that this would not lead to a higher risk of fraud and would be in line with the approach taken as regards the exclusion of merchant initiated transactions (MITs) from the scope of the SCA requirement under PSD2.

22. The EBA is of the view that requiring SCA only once, for the first access, and removing the requirement to apply SCA for subsequent accesses through an AISP would not be in line with the PSD2, and therefore would not be a conceivable option. This is because Articles 97(1)(a) and 97(4) of PSD2 are clear that the requirement to perform SCA also applies when an AISP, acting on the customer's behalf, is accessing the account information. The EBA is of the view that an exemption to SCA that would remove altogether the requirement to apply SCA when an AISP attempts to access the information would not ensure an appropriate level of security of the customer's data, and would therefore not be in line with Article 97(1)(a) of PSD2.

23. As regards the latter argument that had been raised based on the analogy with MITs, the EBA is of the view that this is not a sound argument and is without legal basis. MITs are outside the scope of the SCA requirement because they are payee-initiated payments and, as such, they are not subject to the requirement in Article 97 PSD2 to apply SCA, as clarified in Q&A 2018_4031[4]. By contrast, point (a) of Article 97(2) and Article 97(4) of PSD2 are clear that SCA is required when

[2] https://www.eba.europa.eu/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer-authentication-and-common-and-secure-communication

[3] https://www.eba.europa.eu/eba-publishes-opinion-obstacles-provision-third-party-provider-services-under-payment-services

[4] https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4031

the PSU accesses its account information online, including when the information is accessed through an AISP, which under PSD2 covers both the case where the PSU is actively requesting the information through the AISP and where the AISP is accessing the data without the PSU's involvement (i.e, without the customer actively requesting the information).

3.2.2 The approach proposed in this CP: introducing a new mandatory exemption for cases when the account information is accessed through an AISP and extending the timeline for the renewal of SCA

24. In the CP at hand, the EBA is proposing to:

- Introduce a new exemption to SCA, when an AISP accesses the account information on the PSU's behalf, which on this occasion is mandatory and also subject to certain safeguards and conditions;
- Limit the scope of the voluntary exemption in Article 10 RTS to when the customer accesses the account information directly; and
- Extend the timeline for the renewal of SCA from every 90 to every 180 days, both where the information is accessed through an AISP or directly by the customer.

25. Having discussed these aspects with the European Commission, the EBA understands that there are no legal impediments in the PSD2 to having a mandatory exemption to SCA, provided that the exemption complies with the objectives set out in Article 98(2) PSD2 and with the criteria in Article 98(3) PSD2.

26. Accordingly, the mandatory exemption that is being proposed is accompanied by a number of safeguards and conditions that aim to ensure that the exemption is compatible with the level of risk involved (as required by Article 98(3) PSD2), ensures the safety of the PSU's data, and strikes an appropriate balance between the at times competing objectives of PSD2, such as enhancing the security of payment services, and of promoting user-friendly services on the other.

27. This section explains:

- the safeguards and conditions for the application of the new mandatory exemption;
- its scope of application;
- the extension of the timeline for the renewal of SCA; and
- the implementation timeline.

The safeguards and conditions for the application of the new mandatory exemption

28. In order to address the issues described above, the EBA is proposing to establish a new mandatory exemption to SCA for the case where the account information is accessed through an AISP. The EBA is proposing to make this exemption mandatory for ASPSPs, meaning that ASPSPs would be required *not* to apply SCA where the conditions for the application of the exemption are met.

29. The proposed exemption is subject to a number of safeguards and conditions that ensure that the exemption is compatible with the level of risk involved and meets the PSD2 objective of ensuring the safety of the PSU's data, in accordance with Article 98(2) and (3) of PSD2.

30. In particular, the proposed exemption would only apply where the access is limited to the account balance and/or the most recent 90-day transaction history, without disclosure of sensitive payment data, similarly to the existing exemption in Article 10 RTS. This means that the access to sensitive payment data or to transaction history going back more than 90 days is out of the scope of the exemption, and therefore always requires SCA.

31. Moreover, the exemption would only apply where SCA was applied for the first access to the account information through the AISP, and is renewed periodically, every 180 days. The rationale for choosing the 180 days timeline is explained in more detail in the next sub-section.

32. Furthermore, in order to ensure the safety of the PSU's data, the proposal allows PSPs to revert to SCA at any time if they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access. This may be for example the case where the ASPSP's transaction monitoring mechanisms detect an elevated risk of unauthorised or fraudulent access. In order to ensure a consistent application of the exemption, in cases where ASPSPs revert to SCA on such grounds they should substantiate to their national competent authority, upon request, the reasons for applying SCA. The fact that the ASPSP requires SCA when customers access directly their account information is not in itself a sufficient ground to revert to SCA where the conditions for the application of the mandatory exemption are met.

33. The above is without prejudice to Article 68(5) PSD2, which allows ASPSPs to deny access to a payment account where they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access. In such cases, ASPSPs may either revert to SCA as explained in paragraph 32 above, or deny access to the payment account in accordance with Article 68(5) PSD2.

34. Moreover, in addition to the above safeguards, the PSD2 and the RTS already provide a number of requirements that further mitigate the risk of unauthorised or fraudulent access when an AISP accesses the account information on the customer's behalf. In this regard, it should be noted that AISPs are regulated and supervised entities under the PSD2 that are subject to a number of requirements under the Directive, including the obligations set out in Article 67 of PSD2 to:

    - provide their services only where based on the payment service user's explicit consent;

- identify themselves to the ASPSP through an eIDAS certificate each time they are accessing data, and securely communicate with the ASPSP;

- access only the information from designated payment accounts and associated payment transactions;

- not request sensitive payment data linked to the payment accounts; and

- not use, access or store any data for purposes other than for performing the account information service explicitly requested by the payment service user, in accordance with data protection rules.

35. Furthermore, the risk of unauthorised or fraudulent access is also mitigated by the requirement in Article 2 RTS for PSPs to have in place transaction monitoring mechanisms in order to detect unauthorised or fraudulent payment transactions. As explained above, the ASPSP may revert to SCA at any time where the ASPSP's transaction monitoring mechanisms detect an elevated risk of unauthorised or fraudulent access. Whilst this is not a condition *per se* to the application of the mandatory exemption, the requirement in Article 2 RTS applies more broadly to all PSPs, irrespective of whether or not an exemption is used, and irrespective of whether the exemption is mandatory or voluntary.

The scope of application of the new mandatory exemption

36. To ensure that the proposed amendments to the RTS are proportionate to the issues identified, the EBA is proposing that the new mandatory exemption should apply only when the account information is accessed through an AISP, irrespective of the access interface offered by ASPSPs to AISPs for accessing the account information (i.e, both where the ASPSP offers a dedicated interface, or allows AISPs to use the interfaces used for authentication and communication with its PSUs, in accordance with Article 31 RTS).

37. By contrast, for the other, separate case where customers access the data directly, the EBA is proposing to retain the exemption in Article 10 RTS to be voluntary as is currently the case, as no specific issues have been identified in such cases. However, in order to ensure a level playing field amongst all PSPs, the EBA is also proposing to extend the 90-days timeline for the renewal of SCA to the same 180 days period for the renewal of SCA when the account data is accessed through an AISP, as explained in further detail in paragraph 45 below.

38. The EBA has also considered the alternative option of making the exemption mandatory both when the account information is accessed through an AISP and when customers access directly the account information. However, the EBA has arrived at the view that introducing a mandatory exemption when customers access their account information directly would create an unjustified and disproportionate burden on ASPSPs, mainly for the reason explained above that no particular issues have been raised regarding the application of SCA in such cases. Therefore, the EBA has discarded this latter option.

39. The EBA is of the view that the approach being proposed above, together with the proposal of applying the same timeline for the renewal of SCA of 180-days both for the access through an AISP and when customers access directly the account information (as explained in paragraph 45 below), ensure a level playing field for all PSPs. This is because ASPSPs would also be able to apply the exemption in their direct customer channel should they wish to do so, with the same timeline for the renewal of SCA.

The extension of the timeline for the renewal of SCA

40. As mentioned in paragraph 31 above, one of the conditions for the application of the new mandatory exemption is that SCA is applied for the first access through an AISP, and is renewed periodically every 180 days after that.

41. This means that during the 180-days period, ASPSPs should allow AISPs to access the account information without SCA where the conditions for the application of the mandatory exemption are met. This is without prejudice to the possibility for ASPSPs to revert to SCA at any time if they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access, as explained in paragraph 32 above.

42. The EBA is of the view that the proposed 180-days timeline, combined with the possibility for ASPSPs to revert to SCA in the circumstances mentioned above does not increase the level of risk involved compared to the current 90-days timeline for the renewal of SCA foreseen in the existing Article 10 exemption, and meets the criteria in Article 98(3) PSD2. In the EBA's view, this proposal also strikes an appropriate balance between the current timeline of 90 days which was considered as being too short, and a longer timeline of one year, or more, as suggested by some market participants, which the EBA would consider to be too long from a consumer protection perspective.

43. The EBA also considered the possibility of allowing the PSU to decide how often SCA should be applied for accessing their account information, instead of defining in the RTS a fixed time period for the renewal of SCA. However, the EBA arrived at the view that, whilst such an approach would empower the PSU, it would not be in line with the PSD2. This is because exemptions to SCA set out in the RTS must be objectively defined with clear and unambiguous criteria, in line with the criteria set out in Article 98(3) PSD2, and not on the basis of individual choices of each PSU.

44. Moreover, giving such flexibility to PSUs would go against the PSD2 objective of enhancing security if the time period chosen is not compatible with the level of risk involved. Similarly, such an approach would risk having unintended undesirable consequences as it would lead to a very fragmented and divergent application of the exemption. This would in turn not only fail to address the issues at stake, but may also give rise to more issues for AISPs' services and generate an unproportionate burden for PSPs in applying SCA. For these reasons, the EBA has discarded this option.

45. In order to ensure a level playing field amongst all PSPs, the EBA is also proposing to extend the 90-days timeline for the renewal of SCA in Article 10 RTS to the same 180-days period for the renewal of SCA when the account data is accessed through an AISP. Given that the application of

the Article 10 exemption would remain voluntary for ASPSPs when the customer is accessing the account information directly as explained above, in such cases, ASPSPs would have the possibility, but not the obligation, to apply a timeline for the renewal of SCA of up to 180 days.

46. In the EBA's view, the introduction of a new mandatory exemption for the case where the account information is accessed through an AISP, together with the extension of the timeline for the renewal of SCA to 180 days would:

- mitigate the impact that the issues at hand are having on AISPs' services;
- reduce friction in the customer journey when using AISPs' services;
- ensure a level playing field amongst all PSPs; and
- at the same time, also ensure an appropriate level of security of the PSU's data, for the reasons explained above.

47. The amendments proposed in this CP are those that the EBA is legally in a position to make to address the issues identified. Other mitigations to address other issues are conceivable but would require changes to the Directive itself, which is beyond the EBA's powers to bring about.

Q1. Do you have any comments on the proposal to introduce a new mandatory exemption for the case when the information is accessed through an AISP and the proposed amendments to Article 10 exemption?

Q2. Do you have any comments on the proposal to extend the timeline for the renewal of SCA to 180-days?

The implementation timeline

48. In order to give sufficient time to the industry to implement the necessary changes required to comply with the amending RTS, this CP is proposing a 6-month implementation period after the publication of the final RTS in the Official Journal.

49. As a result, and taking into account the time required for the EBA to assess the consultation responses, for the EU Commission to adopt the RTS, and for the EU Parliament and EU Council to scrutinise the adopted RTS, the amendments are estimated to take effect from Q4 2022 onwards.

50. The CP also provides that, by derogation from the requirements of Article 30(4) RTS, ASPSPs shall make available to AISPs the changes made to the technical specifications of their interfaces required in order to comply with the amending RTS with at least one month ahead of their implementation. This proposal was introduced because, without it, the provisions in Article 30(4) RTS would have required ASPSPs to make available said changes to AISPs with at least 3 months ahead of their implementation, which, taking into account the 6 months implementation period mentioned in paragraph 48 above, would have meant that ASPSPs would have had only 3 months

to adapt their interfaces to meet the new requirements. Since this timeline may be insufficient for ASPSPs, the EBA is proposing to give more time to ASPSPs to adapt their interfaces by allowing them to make available the relevant changes to the technical specifications of their interfaces required to comply with the amending RTS with (at least) one month in advance before such changes are implemented, instead of the 3 months term in Article 30(4) RTS.

51. The proposed derogation from the requirement in Article 30(4) RTS and the one-month timeline proposed above apply only to the changes that ASPSPs are required to make to their interfaces in order to comply with the amending RTS. The proposed derogation and one month timeline do not apply to any subsequent changes that the ASPSP may make to those interfaces, as any such changes would have to comply with Article 30 (4) RTS.

52. The EBA is of the view that the proposed one-month period allows AISPs sufficient time to implement the required changes in their systems and also allows to keep the overall implementation timeline (of 6 months) as short as reasonably possible. This proposal is reflected in Article 2 of the draft amending RTS.

Q3. Do you have any comments on the proposed 6-month implementation timeline, and the requirement for ASPSPs to make available the relevant changes to the technical specifications of their interfaces not less than one month before such changes are required to be implemented?

Draft regulatory technical standards

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

amending the Delegated Regulation (EU) 2018/389 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

(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 the second subparagraph of Article 98(4) thereof,

Whereas:

(1) Article 10 of the Delegated Regulation (EU) 2018/389 provides an exemption from the requirement in 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 such 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 is accessed for the first time, and at least every 90 days after that.

(2) Experience gained during the first years of application of the Delegated Regulation (EU) 2018/389 has shown that the use of this exemption has led to very divergent practices in its application, with some account servicing payment service providers requesting strong customer authentication every 90 days, others at shorter time intervals, whilst a third group have not applied the exemption at all and request strong customer authentication for every account access. This in turn has led to undesirable friction for customers when using account information services, and to a negative impact on the services of account information service providers, particularly in cases where the account servicing payment service provider has implemented a redirection or decoupled approach for carrying out strong customer authentication.

(3) To address these issues and ensure that a proper balance is struck between the objectives of Directive (EU) 2015/2366 of enhancing security of payment services and enabling the development of user-friendly and innovative services, it is necessary to bring further harmonisation in the application of this exemption, for the use case when the account information is accessed through an account information service provider. Accordingly, in such case, payment service providers should not be allowed to choose whether or not to apply strong customer authentication, and the exemption should be made mandatory, subject to certain conditions that are aimed at ensuring the safety of the payment service users' data being met.

(4) To that end, the exemption should be limited to the access to the balance and the recent transactions of a payment account without disclosure of sensitive payment data. Furthermore, the exemption should only apply where strong customer authentication was applied for the first access and is renewed periodically.

(5) Moreover, in order to ensure the safety of the payment service users' data, payment service providers should be allowed to revert to strong customer authentication at any time where they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access. This may be for example 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 substantiate to their national competent authority, upon request, the reasons for reverting to strong customer authentication.

(6) For the case where the payment service user accesses directly the account information, payment service providers should continue to be allowed to choose whether to apply or not strong customer authentication. This is because in such case no particular issues have been observed requiring an amendment to Article 10 exemption, contrary to the case of the access through an account information service provider.

(7) To ensure a level playing field amongst 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 appropriate to establish the same 180-days timeline for the renewal of strong customer authentication for accessing the account information directly with the account servicing payment service provider or through an account information service provider.

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

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

(10) 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[5].

HAS ADOPTED THIS REGULATION:

Article 1

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 and in paragraph 2 of this Article, where a payment service user is accessing its payment account online directly, provided that the access 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 180 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.'

[5] 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, 15.12.2020, p. 12)

(2) A new Article 10a is introduced as follows:

'Article 10a
Access to the payment account information through an account information service provider

1. Payment service providers shall not apply strong customer authentication, subject to compliance with the requirements laid down in paragraph 2 of this Article, where a payment service user is accessing its payment account online through an account information service provider, provided that the access 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 apply 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 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(b) 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 case, the payment service provider shall document and duly justify to its competent national authority, upon request, the reasons for applying strong customer authentication.

Article 2

By way of derogation from Article 30(4) of Delegated Regulation (EU) 2018/389, account servicing payment service providers shall make available to the payment service providers referred to in that Article the changes made to the technical specifications of their interfaces in order to comply with this Regulation not less than one month before such changes are implemented.

Article 3

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.
2. This Regulation shall apply from [*OJ please add date corresponding to 6 (six) months after entry into force date*].
3. This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

For the Commission
The President

[For the Commission
On behalf of the President

Accompanying documents

Draft cost-benefit analysis / impact assessment

Article 10(1) of the EBA Regulation (Regulation (EU) No 1093/2010 of the European Parliament and of the Council) provides that when any draft regulatory technical standards developed by the EBA are submitted to the European Commission for adoption, they shall be accompanied by an analysis of 'the potential related costs and benefits', unless such analyses "are disproportionate in relation to the scope and impact of the draft regulatory technical standards concerned or in relation to the particular urgency of the matter". This analysis should provide an overview of the findings regarding the problem to be dealt with, the solutions proposed and the potential impact of these options.

The following section outlines the assessment of the impact of the proposed amendments to the RTS on strong customer authentication and common and secure open standards of communication.

A. Problem identification

The PSD2 has introduced the requirement to perform SCA with the aim of enhancing security and limiting the risks of fraud. The PSD2 requires SCA to be performed each time a payment service user (PSU) accesses their account online, whether directly or through an account information service provider (AISP).

The RTS provides an exemption (Article 10) from this requirement where customers access, directly or through an AISP, limited payment account information. In such cases, SCA must still be applied when the customer accesses their data for the first time, and at least every 90 days after that. The application of this exemption is voluntary for the account providers (ASPSPs), who can decide whether or not to apply it. This has led to very divergent practices amongst ASPSPs, with some requesting SCA every 90-days, others at shorter time intervals, whilst a third group of ASPSPs have not applied the exemption at all and request SCA for every account access.

The inconsistent application of the exemption has, in turn, led to undesirable friction for customers when using account information services, and to a negative impact on AISPs' services. In particular, this has had a detrimental impact on AISPs that aggregate multiple accounts of the same customer with different account providers, and on AIS use cases that rely on the AISPs' possibility to access the account without the customer being present.

B. Policy objectives

The aim of the changes proposed to the RTS is to address the issues described above, while ensuring the secure access to data.

C. Baseline scenario

The baseline scenario is the scenario in which no changes are made to the current legislation, meaning that the exemption from SCA in Article 10 remains voluntary for ASPSPs, both where customers access the data directly or through an AISP.

Without any changes to the current regulation, it is expected that customers will continue to face friction when using AISPs' services, where ASPSPs do not apply the exemption, or request SCA more frequently than every 90 days. This reduces the convenience for customers of using the services offered by AISPs, and also may have a negative impact on the possibility of AISPs to offer innovative and user-friendly services.

D. Options considered

The following section explains the costs and benefits of some of the options that were considered in order to address the issues described above. Details of the other approaches that had been assessed but discarded because they are not legally feasible under the PSD2 have not been included in this section, but are described in the Rationale section of the CP.

Application of SCA when accessing the data via AISP

Option 1: Optional application of the exemption, with SCA at least every 90 days (status quo)

Option 2: Mandatory application of the exemption, with SCA every 90 days

Option 3: Mandatory application of the exemption, with SCA every 180 days

Application of SCA when the customer accesses its account directly (optional exemption)

Option 1: Optional application of the exemption, with SCA every 90 days (status quo)

Option 2: Optional application of the exemption, with SCA at a lower frequency (180 days or more), in alignment with the frequency of applying of SCA when the access is made through an AISP

E. Cost-Benefit Analysis

This section assesses incremental costs and benefits of the options considered vis-à-vis the baseline scenario.

Application of SCA when accessing the data via an AISP

As an exemption to the requirement in PSD2 that SCA should be applied for each account access, Article 10 RTS, as currently articulated, allows ASPSPs to apply SCA with a frequency of up to every 90 days, both where the customer accesses the data directly or through an AISP.

In cases where AISPs aggregate several accounts of the same customer with different ASPSPs that make use of this exemption, the customer needs to apply SCA at least every 90 days with each ASPSP, with the 90 days cycle for the renewal of SCA with each ASPSP not necessarily overlapping. This means that customers have to perform several SCAs, one with each ASPSP, and often at different points in time, in order to maintain the AISPs' access to those accounts, which creates friction for customers and may deter them from using AISPs' services.

To attenuate this friction, a lower frequency for the application of SCA when the account information is accessed through an AISP could be considered, such as 180 days. Moreover, in order to further mitigate the issues described above, the EBA is proposing to make the application of this exemption to SCA mandatory for the particular case where the information is accessed through anAISP, subject to certain safeguards and conditions being met, that are aimed at ensuring the safety of the customers' data, and which are explained in the Rationale section of the CP. These include the limited scope of data that can be accessed using the exemption, the requirement for the ASPSP to apply SCA for the first access and renew it periodically, and the possibility for the ASPSP to revert, at any time, to SCA if it has objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access. Moreover, the risk of unauthorised access through an AISP is also mitigated by other requirements in the PSD2 and the RTS, including the requirement for AISPs to identify themselves towards the ASPSP through an eiDAS certificate each time they access the account information.

	Costs	Benefits
Option 1: Optional application of the exemption, with SCA at least every 90 days (status quo)	Friction in the customer journey when accessing the data through an AISP Potential moderate to significant costs to AISPs in terms of lost customers and revenues.	No costs to ASPSPs, as no changes required on the ASPSPs side ASPSPs retain the possibility to apply or not the exemption based on their risk assessment
Option 2: Mandatory application of the	In cases where the exemption was not applied before, or was applied at a different frequency, costs related to	Harmonized approach across ASPSPs

exemption, with SCA every 90 days	changes to the authentication procedure and the access interface(s) offered by ASPSPs to AISPs. Depending on the access interface the ASPSP offers to AISPs, this can include the ASPSP's dedicated interface and/or the adapted customer interface(s) in accordance with Article 31 RTS.	Smoother customer experience (compared to cases where the Article 10 exemption is not currently applied). In cases where the exemption was already applied, no additional costs to the ASPSPs. Exceptions still allowed if high-risk, based on transaction risk analysis.
Option 3: Mandatory application of the exemption, with SCA every 180 days	In cases where the exemption was not applied before, or was applied at a different frequency, costs related to changes to the authentication procedure and the access interface offered by ASPSPs to AISPs. Depending on the access interface the ASPSP offers to AISPs, this can include the ASPSP's dedicated interface and/or the adapted customer interface(s) in accordance with Article 31 RTS.	Harmonized approach across ASPSPs Smoother customer experience (compared to cases where the Article 10 exemption is not currently applied) Insignificant increase in risk of fraud. Exceptions still allowed if high-risk, based on transaction risk analysis

Application of SCA when the customer accesses its account directly (optional exemption)

The mandatory exemption that is being proposed in this CP applies only to the access to the account data through an AISP. In cases when the PSU accesses the data directly, the exemption in Article 10 RTS remains voluntary for ASPSPs, who can decide whether or not to apply the exemption.

In order to ensure a level playing field amongst all PSPs, it is proposed to align the 90-days timeline for the renewal of SCA in Article 10 RTS with the 180-days timeline for the case where the account information is accessed through an AISP and the new mandatory exemption applies.

This means that, when the customer is accessing the account information directly, ASPSPs will have the possibility, but not the obligation, to apply a timeline for the renewal of SCA of up to 180 days.

	Costs	Benefits
Option 1: Optional application of SCA every 90 days (status quo)		No additional costs, as no changes required on the ASPSPs side
Option 2: Optional application of SCA at a lower frequency (180 days or more), in alignment with the frequency of application of SCA when connecting via an AISP	If the ASPSPs chooses to apply the exemption, costs related to the changes to the authentication procedure and to the interface(s) used for authentication and communication with the PSUs.	Smoother customer experience Insignificant increase in risk of fraud

F. Preferred option

The preferred option, for the case where the account information is accessed through an AISP, is Option 3. This means that, in such case, the exemption from the application of the SCA will be mandatory for ASPSPs where the conditions for the application of the exemption are met, and SCA will be required every 180 days, unless there is elevated risk of fraud or unauthorised access, in which case the ASPSP can revert at any time to SCA. This option mitigates the impact that the issues at hand are having on AISPs' services and reduces friction in the customer journey when using AISPs' services, while ensuring the security of the customers' data.

For the case where customers access the data directly, it is proposed to keep the exemption in Article 10 optional, but align the frequency of application of SCA to the 180 days timeline for the renewal of SCA when the account data is accessed through an AISP, in order to ensure a level playing field amongst all PSPs.

Overview of questions for consultation

Q1. Do you have any comments on the proposal to introduce a new mandatory exemption for the case when the information is accessed through an AISP and the proposed amendments to Article 10 exemption?

Q2. Do you have any comments on the proposal to extend the timeline for the renewal of SCA to 180-days?

Q3. Do you have any comments on the proposed 6-month implementation timeline, and the requirement for ASPSPs to make available the relevant changes to the technical specifications of their interfaces not less than one month before such changes are required to be implemented?