EBA/RTS/2022/03

5 April 2022

Final Report

Draft Regulatory Technical Standards

amending 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

1. Executive Summary

Article 97 of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) requires payment service providers (PSPs) to apply strong customer authentication (SCA) each time a payment service user (PSU) accesses its payment account online, directly or through an account information service provider (AISP).

By derogation from this requirement, the regulatory technical standards (RTS) on strong customer authentication and common and secure communication (RTS on SCA&CSC) allow PSPs not to apply SCA provided that (i) the access is limited only to the balance of the account and/or the recent transaction history, without disclosure of sensitive payment data; and (ii) SCA is applied when the information is accessed for the first time and at least every 90 days after that.

However, the experience acquired in the application of the RTS has shown that the voluntary nature of this exemption has led to very divergent practices in its application, which have in turn led to friction for customers when using account information services (AIS) and to a negative impact on the provision of these services by third party providers.

In order to address these issues and ensure that a proper balance is achieved between the PSD2 objectives of enhancing security, facilitating innovation and enhancing competition in the EU, the EBA has arrived at the view that there is a need to bring further harmonisation in the application of this exemption, when access to the account information is through an AISP. To this end, the EBA had proposed in the CP published on 28 October 2021 a targeted amendment to the RTS in order to:

- introduce a new mandatory exemption to SCA, for the specific case when access is through an AISP and only if certain conditions are met;
- limit the scope of the voluntary exemption in Article 10 RTS to instances where the customer accesses the account information directly; and
- extend the timeline for the renewal of SCA from every 90 days to every 180 days, both when the information is accessed through an AISP or directly by the customer.

The EBA received more than 1,200 responses to the CP from a wide range of stakeholders. The EBA assessed the feedback received to decide what, if any, changes should be made to the draft amending RTS. In light of the comments received, the EBA agreed with some of the proposals and their underlying arguments and introduced some changes to the draft amending RTS while retaining the mandatory exemption proposed in the CP. In particular, the EBA extended the timeline for ASPSPs to make available to AISPs the changes to their interfaces from 1 month to 2 months before the implementation of these changes and extended the overall implementation period accordingly from 6 months to 7 months after the publication of the amending RTS in the

Official Journal of the EU. Finally, the EBA also introduced some additional clarifications on the application of the mandatory exemption.

Next steps

The draft amending RTS will be submitted to the Commission for endorsement following which it will be subject to scrutiny by the European Parliament and the Council before being published in the Official Journal of the European Union. The amending RTS will apply 7 months after entry into force.

2. Abbreviations

AIS	Account information service
AISP	Account information service provider
API	Application programming interface
ASPSP	Account servicing payment service provider
CP	Consultation paper
EBA	European Banking Authority
EU	European Union
GDPR	Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
NCA	National competent authority
PIS	Payment initiation service
PISP	Payment initiation service provider
PSD2	Payment Services Directive (EU) 2015/2366
PSP	Payment service provider
PSU	Payment service user
RTS	Regulatory technical standards
SCA	Strong customer authentication
SCA&CSC	Strong customer authentication and common and secure open standards of communication
TPP	Third party provider

3. Background and rationale

3.1 Background

1. The revised Payment Services Directive (EU) 2015/2366 (PSD2) 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, 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 (Article 97 PSD2).

2. At the same time, Article 98(1) of PSD2 mandated the EBA to develop regulatory technical standards (RTS) specifying the requirements of SCA and the exemptions from the application of SCA. In developing these requirements, Article 98(2) of PSD2 states that 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. In addition, Article 98(3)(a) PSD2 specifies that exemptions to SCA should be based on the level of risk involved in the service provided.

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&CSC), which were subsequently published in the Official Journal of the EU as an EU Delegated Regulation and are directly applicable across the 27 EU Member States since 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 its payment account information, provided that certain conditions are met, namely:

    - the information accessed is limited to the balance of the account and/or the recent transaction history;

- no sensitive payment data are disclosed; and
- SCA is 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 and through an account information service provider (AISP).

6. When developing the RTS in 2016, the EBA introduced this exemption because, without it, the requirements set out in PSD2 to apply SCA for every single access would have undermined the business viability of account information services, which the PSD2 explicitly sought to promote as a new innovative service in the EU.

7. In line with the legal advice received at the time as to how to interpret the nature of the exemptions that the EBA had been mandated to develop, the EBA construed this exemption, as well as all other exemptions to SCA in the RTS, to be of a voluntary nature. This means that account servicing payment service providers (ASPSPs) are allowed, but not obliged, to use the exemption and at any time can choose to apply SCA to the actions falling within the scope of the exemption. This approach followed the consideration that, in line with Articles 97(5) and 67(2)(b) of PSD2, read together with Recital 30 of PSD2, the PSP applying SCA is the PSP that issues the personalised security credentials, namely the ASPSP. Accordingly, it is the ASPSP that is obliged under PSD2 to perform SCA and bears the liability if it fails to protect the security of the PSU's data and funds. 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, 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, while a third group of ASPSPs have not applied the exemption at all and request SCA for every account access.

9. The inconsistent application of the exemption and the frequent application of SCA have led to undesirable friction for customers and to a negative impact on AISPs' services. This has been particularly the case where the customer uses the services of an AISP to aggregate multiple accounts held with different account providers and has to perform multiple SCAs, one with each account provider and at different points in time, in order to be able to continue using the AISP's services.

10. Moreover, the application of SCA for every single access where the ASPSP does not apply the exemption is limiting certain AIS-use cases that rely on the AISP's ability to access the data without the customer's involvement, such as some personal finance management services and cloud accounting services. This limits the customers' ability to make use of such services and the AISPs' ability to offer its services in the EU single market, contrary to the PSD2 objectives of facilitating innovation and enhancing competition in the EU single market.

11. 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, when the access to account information is done through an AISP. Against this background, and in line with the EBA's mandate in Article 98 PSD2 and Article 8(1)(ka) of Regulation (EU) No 1093/2010[1], the EBA decided to propose a targeted amendment to the RTS, in order to:

    - introduce a new mandatory exemption to SCA, only for the specific case when access is through an AISP and only if certain conditions are met as set out in the draft amending RTS;

    - limit the scope of the voluntary exemption in Article 10 RTS to the case where the customer accesses the account information directly with the ASPSP; and

    - extend the timeline for the renewal of SCA from every 90 days to every 180 days, both where the information is accessed through an AISP or directly by the customer.

12. On 28 October 2021, the EBA published a CP with the above proposed changes to the RTS for a 4-week consultation period. The EBA received a total of 1,278 responses, which provided the EBA with a wide view of all stakeholders, including ASPSPs, AISPs, consumers and corporate users of AIS, technical service providers and API market standardisation initiatives.

13. The EBA has reviewed and assessed the responses and has identified 50 or so distinct issues and requests for clarification that the respondents had raised. The feedback table in Chapter 5 provides an exhaustive list of all these concerns and the respective analysis by the EBA. The Rationale section below, by contrast, focuses on some of the more relevant concerns raised and also explains what, if any, changes the EBA has made to the draft amending RTS as a result. Finally, Chapter 4 presents the final draft amending RTS.

3.2 Rationale

14. The main concerns that were raised by respondents to the consultation related to:

    - the impact of the proposed mandatory exemption on the security of customers' data and funds;

    - the frequency of the renewal of SCA;

    - the implementation period; and

    - transitional provisions in relation to ongoing AISPs' access to the account on the application date of the amending RTS.

[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).

Each of these concerns is addressed below in turn.

15. The EBA has also introduced other less substantive amendments to the draft amending RTS, which are explained in detail in the feedback table at the end of the final report.

3.2.1 The impact of the proposed mandatory exemption on the security of customers' data and funds

16. Some respondents, including some consumers and ASPSPs, raised concerns that a mandatory exemption would remove a layer of security and may lead to increased security risks, as it would not allow ASPSPs to carry out suitable risk and fraud management or apply an appropriate protection level to their customers. They argued that if the ASPSP has decided to apply SCA every time the user accesses an account directly, fraudsters may undermine the ASPSP's security policy by using AISPs for getting access to customers' accounts.

17. By contrast, other consumers and corporate users of AIS as well as AISPs were of the view that the proposed amendments strike a good balance between good user experience and a high level of security. They argued that the cumbersome nature of frequent reauthentication and the different experiences between ASPSPs create friction for customers when using AIS, which leads to customers abandoning AISPs' services. AISPs also argued that this creates an opportunity for market incumbents to reduce the attractiveness of innovative competitors and undermines the objectives of PSD2.

18. The EBA agrees that the security of customers' funds and data is of utmost importance. However, the EBA also recalls that Article 98(2) PSD2 requires the EBA to also take into account, when developing the RTS and the exemptions to SCA, the other key objectives of PSD2 of facilitating innovation and enhancing competition in the EU single market, and to develop the exemptions to SCA based on the criteria established in Article 98(3)(a) PSD2, namely the level of risk involved in the service provided.

19. The EBA believes that the proposed amendments to the RTS strike an appropriate balance between the PSD2 objective of enhancing security, on the one hand, and the innovation and competition enhancing objectives of PSD2, on the other. Furthermore, the EBA believes that the conditions and safeguards that the EBA introduced to accompany the mandatory exemption mitigate the risk of unauthorised or fraudulent access and make the exemption compatible with the level of risk involved.

20. In particular, the EBA recalls that the proposed mandatory exemption only applies to the particular case where an AISP is accessing the limited payment account data specified in Article 10a, without disclosure of sensitive payment data, and under the condition that SCA was applied for the first access to the payment accounts through an AISP and is renewed periodically. Moreover, the ASPSP can, at any time, revert to SCA where it has objective and justified reasons to suspect an unauthorised or fraudulent access in line with the Article 10a(3) RTS or deny access to the payment account in accordance with Article 68(5) PSD2. The choice between applying SCA on the basis of Article 10a(3) or denying access to the payment account

in accordance with Article 68(5) PSD2 will depend on the specific circumstances of the case and the ASPSP's own risk assessment.

21. Furthermore, the EBA would like to emphasise that AISPs are regulated and supervised entities that are subject to security and data protection requirements set out in the PSD2 and other relevant legislation, including:

- the requirement to provide its services only where based on the PSU's explicit consent (Article 67(2)(a) PSD2);
- the prohibition to use, access or store any data for purposes other than for performing the AIS explicitly requested by the PSU in accordance with data protection rules (Article 67(2)(f) PSD2);
- the prohibition to request or access sensitive payment data linked to the payment account (Article 67(2)(e) PSD2 and Article 36 RTS);
- the requirement to securely communicate with the ASPSP and identify themselves towards the ASPSP through a valid eIDAS certificate each time they access the payment account data (Article 67 (2)(c) PSD2 and Article 34 RTS), which mitigates the risk of fraudsters impersonating an AISP in order to gain unauthorised access to the payment account;
- the obligation to ensure that all interactions with the PSU and the ASPSP are traceable, ensuring knowledge *ex post* of all events relevant to the electronic transaction in all the various stages (Article 29 RTS); and
- the requirements in Section 3.4.5b of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) to implement policies and procedures to monitor and detect anomalous activities that may impact information security and to respond to these events appropriately, including, among others, monitoring transactions to detect misuse of access by third parties or other entities.

22. Furthermore, the EBA recalls that all payment or e-money institutions that wish to provide AIS must provide to the relevant NCAs, as part of the authorisation/registration process to be allowed to provide AIS, a security policy document comprising a detailed risk assessment in relation to its payment services and a description of the security control and mitigation measures taken to adequately protect PSUs against the risk of fraud and illegal use of sensitive and personal data (Articles 5(j) and 33 PSD2). The EBA Guidelines on authorisation and registration under the PSD2 (EBA/GL/2017/09) further specify that this security policy document should include, among others:

- the customer authentication procedure used for accessing the account (Section 4.2, guideline 10.1 letter (g)(i));

- a description of the systems and procedures that the applicant has in place for transaction analysis and the identification of suspicious or unusual transactions (Section 4.2, guideline 10.1 letter (g)(iii)); and

- a detailed risk assessment in relation to the payment services the applicant intends to provide, including the risk of fraud, with a link to the security control and mitigation measures explained in the application file, demonstrating that the risks are addressed (Section 4.2, guideline 10.1 letters (a) and (h)).

23. In addition to the above, AISPs are also subject to the requirements in the General Data Protection Regulation (the GDPR), including the obligation in Article 32 of GDPR to ensure the security of the processing of customers' personal data and the accountability principle in Article 24 GDPR.

24. It follows from the above legal requirements that AISPs are responsible for implementing appropriate monitoring mechanisms to detect any attempt of unauthorised or fraudulent access and for taking appropriate measures to mitigate any risk of unauthorised or fraudulent access. This may include for example: (i) taking measures to verify the PSU's identity; (ii) requesting the application of SCA by the ASPSP where the AISP has reasons to suspect an attempt of unauthorised or fraudulent access; and/or (iii) flagging to the ASPSP any suspicion of unauthorised or fraudulent access identified.

25. Finally, the EBA recalls that the PSU can revoke, at any time, the consent given to the AISP to access the account if it no longer wishes the AISP to access the account, at which point the AISP should stop accessing the account in accordance with Article 67(2)(a) PSD2. If the PSU has any concerns that a particular AISP might be accessing its account without consent, the PSU can also convey these concerns to the account provider. In such a case, this would represent justified grounds for the ASPSP to apply SCA to the next access request from the respective AISP in line with Article 10a(3), or deny access to the account in accordance with Article 68(5) PSD2, depending on the specific case and the ASPSP's risk assessment.

26. In view of the foregoing, the EBA has decided to retain the mandatory exemption as proposed in the CP.

3.2.2 The SCA renewal frequency

27. Some respondents raised concerns that the proposed 180-day timeline for the renewal of SCA may increase the risk of unauthorised or fraudulent access during the 180-day period and preferred to retain the current 90-day period in Article 10 RTS. By contrast, other respondents shared the opposite view and suggested increasing this timeline to 1 year or more. These latter respondents argued that a 1-year timeline would be more suitable given the low fraud risk associated with AIS and the safeguards accompanying the new exemption and would also allow AISPs to build up customer loyalty before SCA is required. Some other respondents suggested altogether removing the requirement to renew SCA where the account is accessed through an AISP.

28. Having assessed the arguments presented by these respondents, the EBA has decided to retain the proposed 180-day period for the renewal of SCA. The EBA is of the view that the obligation to renew SCA every 180 days, combined with the ability of ASPSPs to revert at any time to SCA, where they have objective reasons to suspect an attempted unauthorised or fraudulent access, and the other safeguards explained in paragraphs 18 to 25 above strike a good balance between the PSD2 objective of ensuring security, on the one hand, and the innovation and competition enhancing objectives of the PSD2, on the other.

29. With regard to the suggestion made by some respondents to remove the requirement to renew SCA, as explained in the CP, this would not be a feasible option under the PSD2. This is because Articles 97(1)(a) and 97(4) of PSD2 are clear that SCA is required when the PSU accesses its account information online, including 'when the information is requested through an account information service provider'. Therefore, such changes cannot be brought about by amending the RTS, and would require a change to the PSD2 itself, which is not within the EBA's powers to bring about.

3.2.3 The implementation period

30. Some respondents, in particular TPPs, were of the view that the proposed 6-month implementation period is too long and suggested reducing it to 3 months given the urgency of addressing the issues at stake. Other respondents, in particular ASPSPs, shared the opposite view and argued that a 6-month period is too short for them to implement the required changes in its systems and suggested instead extending it to 9months or 1 year. Some of these ASPSPs noted that they would prefer a 1-year timeline not so much because of the complexity of the changes, but rather due to the need to accommodate technology investment decision-making timeframes. They also emphasised that an application date in Q4 2022 would be too short given that budgets for the year 2022 are already closed.

31. Furthermore, some TPPs raised concerns that the proposed 1-month period for making available to TPPs the changes to the technical specifications of ASPSPs' interfaces ahead of implementation is insufficient and would not allow them to understand the technical specifications of all the ASPSPs to which they are connected, discuss these, if necessary, with the respective ASPSPs, and make the necessary changes to their systems. These TPPs asked to retain the standard 3-month period in Article 30(4) RTS for making available to TPPs these changes ahead of implementation by ASPSPs. By contrast, other TPPs were of the view that the proposed 1-month timeline would be feasible for them and indicated that they would not object to this compressed timeline if in return the overall implementation timeline for ASPSPs is also reduced from 6 to 3 months.

32. Having assessed the arguments presented by these respondents, the EBA has decided to extend the period for making available to TPPs the changes to the technical specifications of ASPSPs' interfaces to 2 months before implementation (instead of the 1-month period proposed in the CP, so as to allow sufficient time for TPPs to test and make any necessary changes to their systems before these changes are implemented by ASPSPs. In addition, the

EBA has decided to extend accordingly the application date of the draft amending RTS from 6 to 7 months after the publication of the amending RTS as a Delegated Regulation in the Official Journal of the EU.

33. This means that, after the publication date of the final amending RTS in the Official Journal of the EU, ASPSPs will have:

    a) 5 months to make available to TPPs the documentation with the changes to the technical specifications of its interfaces and allow TPPs to test them in the testing facility; and

    b) 7 months to implement those changes in the production environment.

34. The EBA is of the view that this should give sufficient time to both ASPSPs and AISPs to implement the necessary changes in their systems to comply with the mandatory exemption, make any necessary amendments to the terms and conditions with the PSU in line with Article 54 of PSD2, and duly communicate and explain these changes to PSUs before the application date of the draft amending RTS.

35. These changes are reflected in Articles 2 and 3(2) of the draft amending RTS.

3.2.4 Transitional provisions in relation to ongoing AISPs' access to the account on the application date of the amending RTS

36. A number of respondents sought clarification as to whether AISPs that benefited from the exemption in Article 10 RTS prior to the application date of the amending RTS can continue to access the payment account data without SCA until the expiry of the 90-day period in Article 10 RTS, or whether a new SCA will be required, on the application date of the amending RTS, in order to maintain the AISP's access to the account.

37. In this respect, the EBA clarifies that where ASPSPs have applied the exemption in Article 10 RTS prior to the application date of the amending RTS, they can continue applying that exemption up to 90 days from the last time SCA was applied and request SCA only upon expiry of the 90-day period, without being in breach of the mandatory exemption. This is however without prejudice to the application of the mandatory exemption in Article 10a for new access requests received through an AISP, for which SCA is applied, starting with the application date of the amending RTS.

38. The EBA has also considered the alternative option of requiring ASPSPs to apply the mandatory exemption for all access requests received through an AISP starting with the application date of the amending RTS, and for ASPSPs to request SCA on the application date of the amending RTS in order to maintain the AISPs' access to the account, irrespective of whether the respective AISP had previously benefitted from an exemption under Article 10 RTS.

39. However, the EBA arrived at the view that such latter option may lead to confusion and added friction for PSUs especially if they had just reconfirmed the AISP's access to their account by applying SCA (shortly) before the application date of the amending RTS for another 90-day period, as the PSUs may not understand why they need to apply SCA again. This may also lead to AISPs' connections to the account being inadvertently discontinued if SCA is not applied on the application date of the draft amending RTS. For these reasons, the EBA arrived at the view that a more flexible approach, as outlined above, is preferable. This is now articulated accordingly in Article 3(3) of the draft amending RTS.

4. Draft regulatory technical standards

COMMISSION DELEGATED REGULATION (EU) …/…

of XXX

amending 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 a case, payment service providers are allowed to not 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) 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 achieved between the potentially competing objectives of Directive (EU) 2015/2366 of enhancing security, facilitating innovation and enhancing competition in the European single market, it is necessary to bring further harmonisation in the application of this exemption, 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 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 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 through the respective account information service provider and is renewed periodically.

(5) Moreover, in order to ensure the safety of payment service users' data, payment service providers should, at any time, be allowed to request strong customer authentication if 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 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 or not to apply strong customer authentication. This is because in such cases no particular issues have been observed requiring an amendment to the Article 10 exemption, 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 appropriate to establish the same 180-day 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) 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[2].

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 access is limited to 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] 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. 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 conditions 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 and strong customer authentication was applied.'

(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 access is limited to 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 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 referred to in paragraph 1 for the purpose of the contingency mechanism referred to in Article 33(4), where they do not apply the exemption in Article 10 in the direct interface used for authentication and communication with their payment service users.

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 2 months 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 7 (seven) months after entry into force date*].
3. Payment service providers that applied the exemption in Article 10 of Delegated Regulation (EU) 2018/389 prior to the application date in paragraph 2 shall be allowed to continue applying that exemption up to 90 days from the last time strong customer authentication was applied.
4. 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

5. Accompanying documents

5.1 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 PSU accesses their account online, whether directly or through an 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) that can decide whether or not to apply it. This has led to very divergent practices among ASPSPs, with some requesting SCA every 90 days, others at shorter time intervals, while 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' ability to access the account without the customer being present.

B. Policy objectives

The aim of the draft amending 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 of customers when using the services offered by AISPs, and may also have a negative impact on the ability 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 have been described in the Rationale section of the Consultation Paper.

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 SCA when 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 articulated in the current RTS, 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-day 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, the draft amending RTS provide a lower frequency for the application of SCA when the account information is accessed through an AISP of 180 days. Moreover, in order to further mitigate the issues described above, the draft amending RTS provide that the application of this exemption to SCA is mandatory for the particular case where the information is accessed through an AISP, 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 Final report. These include the limited scope of data that can be accessed using the exemption, the requirement for the ASPSP to apply SCA for first-time access and renew it periodically, and the ability 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 to 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 ability of whether or not to apply 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 changes to the authentication	Harmonised approach across ASPSPs Smoother customer experience (compared to cases where the

exemption, with SCA every 90 days	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) when used as a primary access interface for TPPs in accordance with Article 31 RTS.	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) when used as a primary access interface for TPPs in accordance with Article 31 RTS.	Harmonised 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 included in the draft amended RTS only applies to the access to the account data through an AISP. Where the PSU accesses the data directly, the exemption in Article 10 RTS remains voluntary for ASPSPs, as is currently the case, meaning that the latter can decide whether or not to apply the exemption based on its risk assessment.

In order to ensure a level playing field among all PSPs, the 90-day timeline for the renewal of SCA in Article 10 RTS has been aligned with the 180-day timeline for the renewal of SCA where the account information is accessed through an AISP.

This means that, when the customer is accessing the account information directly, ASPSPs will have the ability, 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 ASPSP's side
Option 2: Optional application of SCA at a lower frequency (180 days), in alignment with the frequency of application of SCA when connecting via an AISP	If the ASPSP 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, where the account information is accessed through an AISP, is Option 3 above (mandatory application of the exemption, with SCA every 180 days). This means that, in such a case, the exemption will be mandatory for ASPSPs subject to the conditions for its application being met, and SCA will be required every 180 days, unless there is an 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.

On the other hand, where customers access the data directly, the exemption in Article 10 will remain optional for ASPSPs, meaning that they can decide whether or not to apply the exemption based on the risk assessment. In addition, in order to ensure a level playing field among all PSPs, the 90-day timeline for the renewal of SCA in Article 10 RTS has been aligned with the 180-day timeline for the renewal of SCA in Article 10a where the account information is accessed through an AISP.

5.2 Views of the Banking Stakeholder Group (BSG)

1. The BSG made a number of comments on the draft amending RTS. The BSG questioned the need to amend the RTS and was of the view that the EBA has not presented concrete evidence identifying the need for such a change. In its view, a more thorough analysis would be necessary to identify if such a change is required by consumers and its impact on the security of the PSUs' data, consumers' privacy and ASPSPs' liability if there is unauthorised or fraudulent access. The BSG argued that it is too early to make such an assessment given that the RTS have been in force for only 2 years and that it took almost a year for ASPSPs to offer dedicated interfaces and use the 90-day exemption.

2. More specifically, the BSG raised concerns that:

- making the exemption mandatory and extending it to 180 days would increase the risk to consumers who are using payment initiation services from the same provider as the account information services;
- the proposed changes may increase the risk that a third party using the same device as the PSU will be able to access the financial data of that PSU, as the ASPSP cannot determine who is using the device;
- a mandatory exemption may be considered as distorting competition and deviating from the principle of 'same activity, same risk, same rules', given that it will mainly benefit one type of PSP, i.e. AISPs;
- technical limitations make a mandatory exemption feasible only for the dedicated interface(s) and not for the customer interfaces.

3. Furthermore, the BSG made the following recommendations:

- to specify in Article 10(3)(a) that the ASPSP can apply SCA at any time if the PSU has requested it;
- to clarify, if a mandatory exemption were to be introduced, that the PSU has the ability to revoke access not only from the AISP, but also from the ASPSP's interface;
- to clarify in Article 2 of the draft amending RTS that ASPSPs should make available to TPPs the changes to ASPSPs' interfaces by providing at least a 1 month's notice before the application date in Article 3(2);
- to consider whether further specification is needed of the definition of 'sensitive payment data', in order to appropriately delimit the scope of the exemption; and

- to ensure that the application date of the draft amending RTS does not require PSPs to make systems changes over the Christmas or New-Year period, given the IT change freezes over that period.

5.3 Feedback on the public consultation and on the opinion of the BSG

The EBA publicly consulted on the draft proposal contained in this final report.

The consultation period lasted for 4 weeks and ended on 25 November 2021. The consultation attracted 1,278 responses, of which 588 gave permission for the EBA to publish them on the EBA website.

This chapter presents a summary of the key concerns and other comments raised by respondents, the analysis and discussion resulting from these comments, and the actions the EBA has taken to address them, if deemed necessary, including changes to the draft amending RTS.

In many cases, respondents made similar comments. In such cases, the comments, and the EBA's analysis thereof, are grouped in a way that the EBA considers most appropriate.

The section below includes the EBA's response to the submission from the EBA's Banking Stakeholder Group. In addition, in the feedback table that follows (pages 30 to 67), the EBA has summarised the comments received from all respondents and has explained which responses have or have not led to changes and the reasons for the decision.

The EBA's response to the Banking Stakeholder Group's submission

1. As described in Section 5.2 above, the BSG made a number of comments on the draft amending RTS.

2. In particular, the BSG questioned the need to amend the RTS and argued that it is too early to assess the need and impact of the proposed changes, given that the RTS have been in force for only 2 years and that it took almost a year for ASPSPs to offer dedicated interfaces and use the 90-day exemption. The EBA disagrees and is of the view that there is a need to make a targeted amendment to the RTS in order to address the issues identified deriving from the inconsistent application of the exemption, as explained in more detail in the CP, and paragraphs 8 to 10 of the Background and Rationale section above. The arguments presented by AISPs as well as some consumers and corporate users of AIS during the public consultation support the EBA's assessment that these issues are creating friction for customers when using AIS and lead to a negative impact on AISPs' services. In particular, the application of SCA for every single access where the ASPSP does not apply the exemption is limiting the AISP's ability to offer some AIS propositions, such as some personal finance management services and cloud accounting services, and the PSU's ability to use such services, contrary to the PSD2 objectives of facilitating innovation and enhancing competition in the EU single market. The EBA

acknowledges that these issues are not the same across all the Member States, but is of the view that the compliance burden that the proposed amendments would entail for ASPSPs needs to be balanced against the key objective of PSD2 of enabling customers to use AIS as an innovative new service across the EU, which objective is currently severely compromised due to the issues identified.

3. The BSG was also of the view that making the exemption mandatory and extending it to 180 days would increase the risk to consumers who are using payment initiation services (PIS) from the same provider offering AIS. The EBA disagrees and recalls that providers of AIS and PIS are regulated and supervised entities that are subject to security and data protection requirements set out in the PSD2 and other applicable EU law, including the General Data Protection Regulation. Where the same provider offers both AIS and PIS, it must comply with the relevant requirements applicable to both services. In particular, the PSD2 is clear that AISPs cannot use, access or store any data for purposes other than for performing the account information service explicitly requested by the PSU in accordance with data protection rules (Article 67(2)(f) PSD2). Also, the PSD2 forbids AISPs to request or access sensitive payment data linked to the payment account (Article 67(2)(e) PSD2 and Article 36 RTS). Moreover, the PSD2 is clear that providers of PIS are not allowed to use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer (Article 66(2)(a)). In addition, Article 97(1)(b) PSD2 requires that SCA is applied for the initiation of an electronic payment transaction, which further mitigates the risk of unauthorised or fraudulent payments being made from the account.

4. The BSG was also of the view that the proposed changes to the RTS may increase the risk that a third party using the same device as the PSU will be able to access the financial data of the PSU. In this respect, the EBA is of the view that this risk is not specific to the proposed amendments to the RTS, nor to the access via an AISP, and that the PSD2 and the RTS already include a number of safeguards to mitigate such risks, including in particular the obligation in PSD2 for PSUs to keep their personalised security credentials safe (Article 69 PSD2). Article 52(5)(a) PSD2 further provides that PSPs should specify in the contract with the PSU the concrete steps PSUs can take in order to keep their personalised security credentials safe. Furthermore, in line with Guideline 3.8 of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), PSPs should establish and implement processes to enhance PSUs' awareness of the security risks linked to the payment services they provide, by offering PSUs with assistance and guidance. In addition, in line with Article 24 RTS, PSPs should ensure that only the PSU is associated with the personalised security credentials and the authentication devices.

5. Furthermore, the BSG was of the view that a mandatory exemption may be considered distorting competition, given that it will mainly benefit one type of PSP, i.e. AISPs. The EBA disagrees and is of the view that, to the contrary, the proposed amendments to the RTS support the PSD2 objective of enhancing competition. In this respect, the EBA notes that all PSPs can rely on the mandatory exemption when acting in their capacity as AISPs, including ASPSPs when acting in their capacity as AISPs with regard to the accounts held by their

customers at other PSPs. Furthermore, in order to ensure a level playing field among all PSPs, the EBA has aligned the 90-day timeline for the renewal of SCA in Article 10 to the same 180-day period for the renewal of SCA when the account data are accessed through an AISP, so as to allow ASPSPs to offer the same exemption to their customers in their direct customer channels.

6. In addition, the BSG argued that technical limitations make the mandatory exemption feasible only for the dedicated interface(s) and not for the customer interfaces. The EBA disagrees and does not find compelling arguments to support such a claim. The EBA recalls that ASPSPs that, in line with Article 31 RTS, have opted to offer access to TPPs via their direct customer interface(s) should have by now adapted their customer interfaces to enable TPPs to identify themselves in accordance with Articles 30(1) and 34 of the RTS. Therefore, where ASPSPs offer access to TPPs via their direct customer interface(s) as a primary access interface in accordance with Article 31 RTS, they should be able to determine whether a request to access the account data comes from an AISP or from the PSU itself, as otherwise they would currently be in breach of law.

7. Regarding the suggestion to specify in Article 10(3)(a) the ability of the ASPSP to revert to SCA if the PSU requests this, the EBA recalls that it is always the PSU who decides whether or not they wish to use the services of an AISP and, if so, what data the AISP can access. At any time, the PSU can revoke the consent given to the AISP to access their account, at which point the AISP is required to stop accessing the data in accordance with Article 67(2)(a) PSD2 and would otherwise be in breach of law. In addition, if the PSU has any concerns that a particular AISP might be accessing their account without consent, the PSU can also convey these concerns to their account provider. In such a case, this would represent justified grounds for the ASPSP to apply SCA to the next access request from the respective AISP in line with Article 10a(3), or deny access to the account in accordance with Article 68(5) PSD2, depending on the specific case and the ASPSP's risk assessment. For these reasons, the EBA does not consider it necessary to further specify in Article 10(3)(a) that ASPSPs can revert to SCA upon request from the PSU.

8. With regard to the suggestion to clarify that the PSU can revoke access not only from the AISP but also from the ASPSP's interface, the EBA notes that the aspects related to contractual consent given by the PSU to the AISP in accordance with Article 67(2)(a), including its revocation, are governed by the PSD2 and are outside the scope of the RTS and of this amendment. In this respect, the European Commission clarified in its answer to Q&A 4309 that 'it is only the PSU that can give consent to the provision of PIS and AIS services. It is consequently also the PSU that only has the right to withdraw the consent after it has been provided. The ASPSP cannot revoke the consent'. This being said, and apart from the issue of revocation of consent given to the AISP, as clarified in paragraph 7 above, if the PSU has any concerns that a particular AISP might be accessing the account without their consent, the PSU can also convey these concerns to their account provider, which can decide accordingly to apply SCA to the next access request from the respective AISP in line with Article 10(3)(a) or deny access to the account in accordance with Article 68(5) PSD2.

9. With regard to the suggestion to refer in Article 2 of the draft amending RTS to the application date in Article 3(2), the EBA clarifies that the wording of Article 2 has been aligned with the wording in Article 30(4) RTS. The timeline for making available to TPPs the changes to ASPSPs' interfaces as per Article 30(4) RTS and Article 2 of the draft amending RTS is a separate issue to the application date of the draft amending RTS. For these reasons, the EBA does not consider that further changes to the wording in Article 2 of the draft amending RTS are needed.

10. With regard to the suggestion to further specify what constitutes 'sensitive payment data', the EBA recalls that this concept is defined in Article 4(32) of PSD2. Therefore, such change cannot be brought about by amending the RTS, and would require a change in the PSD2, which is not within the EBA's powers to bring about.

11. Finally, regarding the suggestion to ensure that the application date of the draft amending RTS does not require PSPs to make system changes over the Christmas period, the EBA clarifies that the application date of the draft amending RTS will depend on the legislative process for its adoption by the EU Commission and the EU Parliament and Council, which is not within the EBA's control.

Summary of responses to the consultation and the EBA's analysis

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	Responses to questions in the Consultation Paper		
	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?		
1	Some respondents disagreed with the proposed amendments and were of the view that the EBA has not presented concrete evidence to justify the need to amend the RTS. Several of these respondents argued that the decline in AISPs' customers is not due to the SCA renewal, but rather to the fact that customers no longer wish to use AISPs' services. Some respondents also argued that it is too early to assess the necessity and impact of the proposed changes given that the RTS have been in force for only 2 years and that it took almost a year for ASPSPs to offer dedicated interfaces and use the 90-day exemption. They suggested that instead these issues should be considered as part of the upcoming PSD2 review, in order to avoid the risk that ASPSPs would be required to implement a mandatory exemption for a potentially very short application period, should a different assessment of this exemption be made as part of the PSD2 review. Other respondents were of the opposite view and strongly supported the proposed amendments to the RTS. They argued that the need to apply SCA every 90 days (or more frequently) combined with poorly	Having assessed the arguments presented by these respondents, the EBA is still of the view that there is a need to make a targeted amendment to the RTS in order to address the issues arising from the inconsistent use of the exemption in Article 10 RTS, as explained in more detail in the CP and paragraphs 8 to 10 of the Background and Rationale section above. The arguments presented by AISPs as well as some consumers and corporate users of AIS during the public consultation supports the EBA's assessment that these issues are creating friction for customers when using AIS and lead to a negative impact on AISPs' services. In particular, the application of SCA for every single access where the ASPSP does not apply the exemption limits the AISP's ability to offer certain AIS-use cases, such as some personal financial management services and cloud accounting services, and the PSU's ability to use such services, contrary to the PSD2 objectives of facilitating innovation and enhancing competition in the EU single market.	None.

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	designed SCA workflows deployed by ASPSPs have led to a poor customer experience, and that as a result, AISPs are facing significant abandonment rates, that are endangering the commercial viability of AIS in the EU. In this respect, one TPP trade association reported that up to 50% of the customer base of its members offering AIS are abandoning their AISP service every 90 days when SCA is requested. Similarly, another TPP trade association reported that TPPs' attrition rates typically range from 20-40% every 90 days when SCA is required, while a third TPP trade association argued that TPPs are facing customer attrition rates between 13 and 65%, depending on the business model, every 90-days when SCA is required. The latter trade association also reported that in cases where the ASPSP requires SCA for every data access by the AISP, this results in a near 100% customer attrition rate for the TPP, making such AIS-use cases commercially unviable. This is the case for example of AIS propositions that rely on the AISP's ability to access the data without the customers actively requesting that data, such as some personal financial management services that offer budget and financial dashboards and cloud accounting services that keep real-time records of business banking transactions.	The EBA acknowledges that these issues are not the same across all the Member States, but is of the view that the compliance burden that the amendments to the RTS would entail for ASPSPs needs to be balanced with the key objective of PSD2 of enabling customers to use AIS as an innovative new service across the EU, which objective is currently severely compromised due to the issues identified. Finally, in response to the view that these issues should not be addressed by amending the RTS, but in the upcoming review of the PSD2 Directive, the EBA notes that no decision for a revision of PSD2 has yet been made by the EU Commission and, if it is made, it will take 4 to 6 years for a revised Directive to be proposed, negotiated and transposed. The EBA therefore sees no risk of ASPSPs having to implement mandatory exemptions for a very short time only, as some respondents have indicated.	
2	Some respondents were of the view that a mandatory exemption could lead to increased security risks as it would not allow ASPSPs to carry out suitable risk and fraud management, or to apply an appropriate protection level to their customers. These respondents argued that a mandatory exemption would not be in line with Article	The EBA agrees that the security of customers' funds and data is of utmost importance. However, the EBA also recalls that Article 98(2) PSD2 requires the EBA to also take into account, when developing the RTS and the exemptions to SCA, the other key objectives of PSD2 of facilitating	None.

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	1 RTS as it would not allow ASPSPs to decide whether or not to apply an exemption based on their risk assessment. Other respondents were of the view that the proposed amendments could indirectly lead to an increased risk of fraud as fraudsters could repeatedly gain unauthorised access to the payment account data during the 180-day period. These respondents noted that an increasing number of fraud cases are linked to fraudsters gaining access to detailed data and information about a customer (via social engineering) and impersonating the bank in front of the customer, who will rely on them due to the nature of the concrete piece of information they possess. Other respondents commented that, if a mandatory exemption were to be introduced for access through an AISP, fraudsters could undermine ASPSPs' security policy by using AISPs to access customers' accounts.	innovation, and enhancing competition in the EU single market, and to develop the exemptions to SCA based on the criteria established in Article 98(3)(a) PSD2, namely the level of risk involved in the service provided. The EBA believes that the proposed amendments to the RTS strike an appropriate balance between the PSD2 objective of ensuring security, on the one hand, and the innovation and competition enhancing objectives of the PSD2 on the other. Furthermore, the EBA believes that the conditions and safeguards that it introduced to accompany the mandatory exemption mitigate the risk of unauthorised or fraudulent access and make the exemption compatible with the level of risk involved. In particular, the EBA recalls that the mandatory exemption applies only when an AISP is accessing the limited payment account data specified in Article 10a, without disclosure of sensitive payment data, and provided that SCA was applied for the first access through the respective AISP and is renewed periodically. Moreover, the ASPSP can, at any time, revert to SCA where it has objective and justified reasons to suspect unauthorised or fraudulent access in line with Article 10a(3) RTS, or deny access to the payment account in accordance with Article 68(5) PSD2. Furthermore, the EBA would like to emphasise that AISPs are regulated and supervised entities that are subject to security and data protection requirements set out in the PSD2 and other relevant legislation, including:	

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		• the requirement to provide their services only where based on the PSU's explicit consent (Article 67(2)(a) PSD2); • the prohibition to use, access or store any data for purposes other than for performing the AIS explicitly requested by the PSU in accordance with data protection rules (Article 67(2)(f) PSD2); • the prohibition to request sensitive payment data linked to the payment account (Article 67(2)(e) PSD2 and Article 36 RTS); • the requirement to securely communicate with the ASPSP and identify themselves towards the ASPSP through a valid eIDAS certificate each time they access the payment account data (Article 67 (2)(c) PSD2 and Article 34 RTS), which mitigates the risk of fraudsters impersonating an AISP in order to gain unauthorised access to the payment account; • the obligation to ensure that all interactions with the PSU and the ASPSP are traceable, ensuring knowledge *ex post* of all events relevant to the electronic transaction in all the various stages (Article 29 RTS); and • the requirements in Section 3.4.5b of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) to implement policies and	

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		procedures to monitor and detect anomalous activities that may impact their information security and to respond to these events appropriately, including, among others, monitoring transactions to detect misuse of access by third parties or other entities. Furthermore, the EBA recalls that all payment and e-money institutions that wish to provide AIS must provide to their NCAs, as part of the registration/authorisation process to be able to provide AIS, a security policy document comprising a detailed risk assessment in relation to their payment services and a description of the security control and mitigation measures taken to adequately protect PSUs against the risk of fraud and illegal use of sensitive and personal data (Articles 5(j) and 33 PSD2). The EBA Guidelines on authorisation and registration under the PSD2 (EBA/GL/2017/09) further specify that this security policy document should include among others: • the customer authentication procedure used for accessing the account (Section 4.2, Guideline 10.1 (g)(i)); • a description of the systems and procedures that the applicant has in place for transaction analysis and the identification of suspicious or unusual transactions (Section 4.2, Guideline 10.1 (g)(iii)); and	

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		• a detailed risk assessment in relation to the payment services the applicant intends to provide, including the risk of fraud, with a link to the security control and mitigation measures explained in the application file, demonstrating that the risks are addressed (Section 4.2, Guideline 10.1 (a) and (h)). In addition to the above, AISPs are also subject to the requirements in the General Data Protection Regulation (the GDPR), including the obligation in Article 32 GDPR to ensure the security of the processing of customers' personal data and the accountability principle in Article 24 GDPR. It follows from the above legal requirements that AISPs are responsible for implementing appropriate monitoring mechanisms to detect any attempt of unauthorised or fraudulent access and for taking appropriate measures to mitigate any risk of unauthorised or fraudulent access. This may include for example: (i) taking measures to verify the PSU's identity; (ii) requesting the application of SCA by the ASPSP where the AISP has reasons to suspect an attempt of unauthorised or fraudulent access; and/or (iii) flagging to the ASPSP any suspicion of unauthorised or fraudulent access identified. Furthermore, the EBA recalls that PSUs can revoke, at any time, the consent given to the AISP to access the account if they no longer wish the AISP to access their account, at	

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		which point the AISP is required to stop accessing the account in accordance with Article 67(2)(a) PSD2 and would otherwise be in breach of law. If the PSU has any concerns that a particular AISP might be accessing the account without their consent, the PSU can also convey these concerns to their account provider. In such a case, this would represent justified grounds for the ASPSP to apply SCA to the next access request from the respective AISP in line with Article 10(3)(a) or deny access to the account in accordance with Article 68(5) PSD2, depending on the specific case and the ASPSP's risk assessment. In view of the foregoing the EBA has decided to retain the mandatory exemption as proposed in the CP.	
3	Some respondents were of the view that a mandatory exemption would increase the risk that when a user downloads a token on a device, any other individual using the same device will be able to access the PSU's financial data, as the ASPSP cannot determine who is actually using the device. Respondents argued that this will make PSUs more dependent on the security levels of the device used for accessing their account.	The EBA is of the view that this is a general security risk that is not specific to this amendment to the RTS, nor to the access via an AISP, and that the PSD2 and the RTS already provide a number of safeguards to mitigate such risks. In particular, the obligation to keep personalised security credentials safe is of utmost importance in order to limit such risks. In this respect, the PSD2 requires PSUs to take all reasonable steps to keep their personalised security credentials safe (Article 69 PSD2). Furthermore, Article 52(5)(a) PSD2 provides that PSPs should specify in the contract with the PSU the concrete steps that PSUs can take in order to keep their personalised security credentials safe. Also, in line with Guideline 3.8 of the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), all PSPs,	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		including both ASPSPs and AISPs, should establish and implement processes to enhance PSUs' awareness of the security risks linked to the payment services they provide, by providing PSUs with assistance and guidance. In addition, in line with Article 24 of the RTS, PSPs should ensure that only the PSU is associated with the personalised security credentials and the authentication devices. In this respect, Q&As 4560 and 4561 provide further clarifications on the use of an authentication device by multiple users, including the association of the personalised security credentials.	
4	Some respondents argued that the proposed amendments exceed the EBA's mandate set out in Article 98 PSD2. They argued that a mandatory exemption is not actually an exemption but reverses the default rule in Article 97 PSD2 by forbidding PSPs to apply SCA for access to the payment account within the 180-day period. In their view, such changes would require an amendment of the PSD2 by the EU co-legislators and may be seen as a political orientation, aimed at giving an advantage to TPPs and goes contrary to Article 10 of the EBA Regulation which specifies that: 'Regulatory technical standards shall be technical, shall not imply strategic decisions or policy choices and their content shall be delimited by the legislative acts on which they are based'. Furthermore, some respondents argued that setting a mandatory exemption would require the EBA to make the *ex ante* assumption that the risk level will always be low where an AISP is used, which goes	The EBA is of the view that the amendments to the RTS are in line with the EBA's mandate as set out in Article 98 PSD2. Article 98 PSD2 mandated the EBA to develop RTS specifying the requirements of SCA and the exemptions from the application of SCA, which the EBA has done by developing the RTS on SCA&CSC that were subsequently published in the Official Journal of the EU as Commission Delegated Regulation (EU) 2018/389 and apply as of 14 September 2019. The proposed mandatory exemption is in line with Article 98(1)(b) PSD2 which mandated the EBA to develop exemptions to SCA. Additionally, the PSD2 requires the EBA to draft the exemptions to SCA based on the criteria established in paragraph 3(a) of that article, namely the level of risk involved in the service provided. Taking into	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	contrary to the requirements in Article 1(b) RTS and Article 98(3) PSD2.	account the conditions and safeguards accompanying the mandatory exemption (explained in more detail in the response to comment 2 above), the EBA is of the view that the exemption is compatible with the level of risk involved and therefore complies with the criteria in Article 98(3)(a) PSD2. Moreover, the proposed amendments are also in line with Article 98(5) PSD2 which provides that the EBA shall review and, if appropriate, update the RTS on a regular basis in order, *inter alia*, to take account of innovation and technological developments, and Article 8(1)(ka) of Regulation (EU) No 1093/2010 (the EBA Founding Regulation) which provides that the EBA shall regularly update all its regulatory technical standards.	
5	Some respondents sought clarifications regarding the liability of ASPSPs in the context of the mandatory exemption. Others commented that the allocation of liabilities and risks in the PSD2 is not fairly balanced between ASPSPs and PISPs/AISPs and that the proposed amendments would worsen this unbalance, as the ASPSP would still be liable. They suggested that the entity that benefits from the SCA exemption (in this case, AISPs) should bear the burden of proof and manage the relationship with the customer if there are any complaints.	The allocation of liability between ASPSPs and TPPs, including in relation to the liability vis-à-vis the PSU, is regulated in the PSD2 and falls outside the scope of the RTS and therefore also of this amendment to the RTS.	None
6	Some respondents were of the view that the proposed amendments are distorting competition as they will benefit only one type of PSPs,	The EBA disagrees and is of the view that these amendments to the RTS will help ensure a level playing field	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	i.e. AISPs, and are deviating from the principle of 'same activity, same risk, same rules'.	between all market players offering AIS across the EU and support the PSD2 objective of enhancing competition. In this respect, the EBA notes that all PSPs, can rely on the mandatory exemption when acting in their capacity as AISPs, including ASPSPs when acting in their capacity as AISPs with regard to the accounts held by their customers at other PSPs. Furthermore, in order to ensure a level playing field among all PSPs, the EBA has aligned the 90-day timeline for the renewal of SCA in Article 10 exemption to the same 180-day period for the renewal of SCA when the account data are accessed through an AISP so as to allow ASPSPs to offer the same exemption to their customers in their direct customer channels.	
7	Some respondents argued that the proposed mandatory exemption is not in line with Article 67(3)(b) PSD2, because it would prevent ASPSPs from applying SCA when the PSU accesses its payment account(s) through an AISP, while the ASPSP may decide to require SCA each time PSUs access their account information directly.	The EBA disagrees and recalls that Article 67(3)(b) PSD2 requires ASPSPs to 'treat data requests transmitted through the services of an AISP without any discrimination for other than objective reasons'. The application of the mandatory exemption does not lead to more unfavourable treatment of data requests transmitted through an AISP compared to the case where the PSU is directly accessing the data – on the contrary, the mandatory exemption may lead to a better customer experience when using an AISP, which is in line with Article 67(3)(b) PSD2. As explained in paragraphs 38-39 of the CP, when developing the draft amending RTS, the EBA had also	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		considered the option of making the exemption mandatory both when the account information is accessed through an AISP and when PSUs directly access their account information online with the ASPSP. However, the EBA has arrived at the view that making the exemption mandatory in the latter case would create an unjustified and disproportionate burden on ASPSPs, as no particular issues have been raised regarding the application of SCA in such cases. Therefore, the EBA has retained the voluntary nature of the exemption in Article 10 RTS for the case where customers directly access their account with the ASPSP.	
8	One respondent was of the view that PSUs may become confused if faced with different user experiences regarding the application of SCA when accessing their accounts directly compared to when they use an AISP. The respondent was of the view that the less PSUs understand whether or not they are expected to provide SCA, the more vulnerable they are to both phishing and social engineering attacks. The respondent suggested that consistent application of SCA by the ASPSP, regardless of whether the account is accessed directly or through an AISP, would strengthen the PSU's security.	The EBA reiterates that the application of the exemption in Article 10 remains voluntary for ASPSPs when PSUs directly access their account information online with the ASPSP, as it is currently the case. As explained in the response to comment 7 above, when developing the draft amending RTS the EBA had also considered the option of making the exemption mandatory both when the account information is accessed through an AISP and when PSUs directly access their account information online with the ASPSP. However, the EBA has arrived at the view that making the exemption mandatory in the latter case would create an unjustified and disproportionate burden on ASPSPs, as no particular issues have been raised regarding the application of SCA in such cases.	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
9	Some respondents were of the view that the proposed amendments are not technological neutral and will lead to an uneven playing field between ASPSPs that offer a dedicated interface (such as an API) and those that offer access to TPPs via their customer interfaces in line with Article 31 RTS. These respondents argued that, where the ASPSP has opted to offer access to TPPs via its customer interface, it would be technically very difficult, or even impossible, to differentiate between the access by an AISP and the direct access by the PSU, and that, as a result, these ASPSPs will have to comply with the mandatory exemption also in their direct relationship with their customers and will not be able to invoke the optional exemption in Article 10. One respondent also argued that the changes that these ASPSPs would need to make to their customer interfaces in order to comply with the mandatory exemption would require the same level of investments as an API (as regards access to the account data) and that this would indirectly leave no choice to those ASPSPs but to develop an API, which goes against Article 31 RTS. The respondent suggested that either the mandatory exemption should not apply when an ASPSP decides to offer access to TPPs via its customer interface, or the ASPSP should be allowed to charge for access to the data.	The EBA disagrees and recalls that, in accordance with Article 30(1) RTS, ASPSPs should ensure that TPPs are able to identify themselves to the ASPSP, irrespective of whether the ASPSP has opted to offer a dedicated interface or to allow TPPs to use the same interfaces used for authentication and communication with the ASPSP's PSUs. Therefore, ASPSPs that in line with Article 31 RTS have opted to offer access to TPPs via their customer interface(s) should have already by now adapted those interfaces to enable TPPs to identify themselves and should be able to determine whether a request to access the account data comes from an AISP or from the PSU itself, as otherwise they would currently be in breach of law. Therefore, the mandatory exemption does not prejudice the choice that ASPSPs have under Article 31 of the RTS between offering a dedicated interface and allowing TPPs to use the ASPSP's direct customer interfaces, or the ability of ASPSPs that have chosen the latter option to decide whether or not to apply the voluntary exemption in Article 10 in their direct relationship with their customers.	None
10	A few respondents sought clarifications on whether ASPSPs that offer a dedicated interface and that have not been exempted from the requirement to establish the contingency mechanism in Article 33(4) RTS should also implement the mandatory exemption in their direct customer channels for the purpose of the contingency mechanism.	The EBA clarifies that ASPSPs that offer a dedicated interface and have not received an exemption from the requirement to set up the contingency mechanism in Article 33(4) RTS are not required to implement the mandatory exemption in their direct customer interfaces for the purpose of the contingency mechanism, if they do	A new Article 10a (4) is introduced as follows: 'Account servicing payment service providers that offer

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	These respondents were of the view that banks that offer a dedicated interface and have not received an exemption from establishing the fallback mechanism should only be required to implement the mandatory exemption in their dedicated interface, and not their fallback interface. One of these respondents argued that adapting both interfaces would require extensive technical changes, tests and security reviews (especially for the fallback) and that having only 6 months to adapt systems to these new requirements would introduce major risks in maintaining stable and secure banking services.	not use the exemption in Article 10 in their direct customer channels. In this respect, the EBA recalls that the contingency mechanism in Article 33(4) RTS should be used only as an emergency and temporary access mechanism, until the dedicated interface is restored to the level of availability and performance provided for in Article 32 RTS. The EBA is of the view that it would be disproportionate to require ASPSPs that offer a dedicated interface to also implement the mandatory exemption in their customer interfaces (in addition to implementing the exemption in their dedicated interface) for the purpose of the contingency mechanism in Article 33(4) RTS if these ASPSPs do not use the exemption in Article 10 in their direct customer channels. By contrast, if the ASPSP applies the exemption in Article 10 in its direct customer channels, it should also apply the exemption where AISPs use the customer interface as a fallback access in accordance with Articles 33(4) and (5) RTS and Article 67(3)(b) PSD2. This has been clarified in paragraph 4 of Article 10a.	a dedicated interface as referred to in Article 31 shall not be required to implement the exemption referred to in paragraph 1 for the purpose of the contingency mechanism referred to in Article 33(4), where they do not apply the exemption in Article 10 in their direct interface used for authentication and communication with their payment service users'.
11	Some respondents were of the view that the requirement to apply SCA in PSD2 does not apply when the AISP accesses the payment account information without the customer actively requesting that data. In support of this view, respondents argued that:	The EBA clarifies that Article 97(2)(a) and Article 97(4) of PSD2 require SCA when the PSU accesses its account information online, including 'when the information is requested through an account information service	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	- Article 97(1)(a) PSD2 provides that SCA applies 'where the payer accesses its payment account online', and does not say 'where the payer accesses its online payment account', which implies that SCA applies when the payer is online; - Article 97(4) PSD2 provides that SCA applies 'when the information is requested through an AISP', and does not say when the 'information is requested by an AISP'; - Based on Article 36(5)(b) of the RTS, the access by an AISP to the account information without the customer's involvement is not an instance of the payer accessing its payment account online (that requires SCA under PSD2), but instead an instance of the AISP (and not the payer) accessing the payment account online, that does not require SCA under PSD2; - The above AIS-use case (where the AISP accesses the payment account information without the customer actively requesting that information) is not captured by the SCA requirement in Article 97 PSD2 because it was not envisaged at the time the PSD2 was adopted; There is very little risk when an AISP accesses the data, and therefore it is reasonable and proportional to not require SCA when the AISP accesses the data without the customer's involvement, considering also that there are other security measures in PSD2 that apply to AISPs, such as the requirement to securely communicate with the ASPSP and identify themselves via an eIDAS certificate and the registration/authorisation requirements in the PSD2.	provider'. This includes both the case where the PSU is actively requesting the information through an AISP and the case where the AISP is accessing the payment account data without the PSU's active involvement, as the text in the PSD2 does not distinguish between these two scenarios.	

No.	Summary of responses received	EBA analysis	Amendments to the proposals
12	Some respondents were of the view that instead of imposing a mandatory exemption and requiring SCA renewal at a predetermined frequency in all cases, the PSU should be allowed to decide if an exemption should apply or not for a given AISP on an individual basis, as well as, where applicable, the frequency for applying SCA.	As explained in paragraphs 43 and 44 of the CP, when developing the draft amending RTS, the EBA had also considered the possibility of allowing the PSU to decide how often SCA should apply when using the services of an AISP. However, the EBA discarded such an approach because 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, based on the criteria in Article 98(3) PSD2, and cannot be defined based on individual choices of each PSU. Furthermore, such an approach may go against the PSD2 objective of enhancing security if the time period chosen by the PSU for the renewal of SCA is not compatible with the level of risk involved. Moreover, this could lead to very divergent practices in the application of SCA that would generate an unproportionate burden for all PSPs in applying SCA and would further exacerbate the issues faced by AISPs. For these reasons, the EBA has discarded this option.	None
13	Some respondents suggested removing the requirement to apply SCA where customers access the account information through an AISP and instead require customers to confirm periodically to the AISP that they still wish to continue using their service. A few respondents suggested not requiring any SCA renewal or any confirmation of consent to the AISP, and require only a single SCA when the customer first uses the AISP's services. These respondents argued that:	As explained in paragraphs 21 to 23 of the CP, removing the requirement to apply SCA when an AISP accesses the payment account information is not a feasible option under the PSD2. This is because Articles 97(1)(a) and 97(4) of PSD2 are clear that SCA is required when the PSU accesses its account information online, including 'when the information is requested through an account information service provider'. Therefore, such changes cannot be	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	- the friction introduced by SCA is disproportionate to the low risk of AIS and leads to a poor customer experience and high customer abandonment rates for AISPs; - at any time, PSUs can stop access to their account information directly with the AISPs; - AISPs are regulated entities subject to the security requirements in PSD2 and are also subject to data protection requirements under the GDPR, and already provide strong consumer protection with regard to the access to data; - customers do not understand why the renewal of SCA is imposed if the AISP is licensed; - SCA increases the risk of customers' security information being exploited by hackers each time a customer is asked to authenticate. Also, one respondent suggested that, as an alternative to requiring SCA renewal, the EBA should require AISPs to notify the PSU about the active AIS connections, for example every 180 days, and offer the option to the PSU to easily terminate the AIS connection. The respondent argued that this would mitigate the risk that PSUs may unintentionally keep a bank account connected for a longer period of time than desired.	brought about by amending the RTS, and would require a change of the PSD2, which is not within the EBA's powers.	
14	One respondent suggested that the EBA should consider differentiated SCA requirements for corporate PSUs and relieve corporate PSUs from the requirement to renew SCA. Said respondent noted that the EBA refers in paragraph 42 of the CP to the 'consumer	The EBA recalls that the requirement in Article 97(1) PSD2 to apply SCA applies to all PSUs, irrespective of whether they are natural or legal persons. The EBA does not find compelling arguments to provide a differentiated	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	protection perspective' and was of the view that there are fundamental differences in perspectives of consumers and corporations with regard to protection requirements.	exemption to SCA for corporate PSUs as regards access to the payment account data. The reference in paragraph 42 of the CP to the 'consumer protection perspective' was not intended to suggest otherwise.	
15	Some respondents suggested that customers should not be required to reauthenticate with each ASPSP and for each bank account, and that instead, in order to allow for a better customer experience, the AISP should be responsible for the renewal of SCA on the ASPSP's behalf.	As explained in paragraphs 19 and 20 of the CP, a mandatory delegation of SCA to AISPs in order for the latter to perform SCA on the ASPSP's behalf is not possible under the PSD2 and would require a change of the PSD2, which is not within the EBA's powers to bring about. 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. While 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.	None
16	One respondent suggested that PSUs should be allowed to mandate other persons (e.g. an adviser, lawyer, accountant, etc.) to perform SCA on their behalf. The respondent argued that this would be particularly beneficial for some AIS-use cases, such as cloud accounting services, and referred to anecdotal data reported by accountants claiming that some of their customers (SMEs) would rather share log-in credentials with accountants in order for the latter to perform SCA on the SMEs' behalf, than log in every 90 days themselves to perform SCA.	The EBA notes that the granting of such a mandate, while potentially possible based on contractual arrangements, is outside the scope of the PSD2 and of the RTS, and therefore also outside the scope of this amendment to the RTS.	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	Moreover, the respondent argued that it is unnecessarily burdensome for PSUs to reauthenticate with the ASPSP when they have authenticated with the TPPs' application and continue to directly access their account transactions in the TPP's application.		
17	Some respondents were of the view that the proposed mandatory exemption should not be limited to AISPs only and that it should also apply to account information access requests by payment initiation service provider (PISPs) in order to maintain fair competition among all PSPs. These respondents argued that (i) the current Article 10 does not limit the SCA exemption to AISPs only, and that (ii) there are legitimate payment account information access use cases that form part of current PISP customer journeys, for example, when the payer is required to review payment account information and select an account to be debited in the ASPSP's domain. These respondents suggested replacing the reference to AISPs in Article 10a with a reference to 'payment account access online through an authorised payment service provider'.	The EBA disagrees and notes that a PSP that is authorised to provide PIS but not AIS is not authorised to access the customer's payment account data referred to in Article 10 RTS and therefore cannot rely on the exemption in Article 10 RTS to do so. In the scenario referred to by the respondents, where the payer selects as part of a PIS journey the payment account to be debited from a list of payment accounts in the ASPSP's domain, the respective list of accounts is displayed by the ASPSP only to the PSU. A PSP that is authorised to provide payment initiation services but not AIS is not authorised to access the respective list of accounts. As clarified in paragraphs 38 to 40 of the EBA Opinion on obstacles under Article 32(3) of the RTS (EBA/OP/2020/10), 'the ASPSP is not required to share with PISPs the list of all the PSU's payment accounts. In fact, a PISP is not entitled under PSD2 to access the list of all the PSU's payment accounts, as this information goes beyond the scope of data that PISPs have the right to access under Article 66(4)(b) PSD2 and Article 36(1)(b) RTS'. Accordingly, the Opinion clarified that 'not providing the list of all payment accounts to a PISP is not an obstacle', and also that 'where the PISP does not communicate to the ASPSP the IBAN of the PSU account to	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		be debited, and the PSU selects the account on the ASPSP's domain, the ASPSP should provide to the PISP the number of the account that was selected by the PSU and from which the payment was initiated, in accordance with Article 66(4)(b) of PSD2 and Article 36(1)(b) RTS, if this information is also provided or made available to the PSU when the payment is initiated directly by the PSU'.	
18	One respondent argued that, in order to ensure a level playing field, AISPs should also be required to request their PSUs to perform SCA if they want to show a transaction history older than 90 days or any sensitive payment data when the PSU accesses this data in the AISP's own channels/app. The respondent was of the view that, since AISPs are not required to request SCA when the customer accesses the data in the AISP's channels, the PSU as well as any other person accessing the PSU's account on the AISP's interface (possibly including fraudsters) will have access to the whole transaction history previously retried and stored by the AISP without any SCA.	The application of SCA by AISPs in their own channels goes beyond the scope of this amendment. The issue has been submitted to the EBA via the EBA's Q&A tool as Q&A 6248 and will be answered there.	None
19	Some respondents argued that TPPs are facing unfair competition because some ASPSPs are offering commercial or 'premium' APIs that do not require SCA renewal and that offer superior account information services compared to the PSD2 dedicated interfaces offered to AISPs. Some respondents referred in particular to the Electronic Banking Internet Communication Standard (EBICS) T interface which allows access to bank account information. They argued that when a client accesses account information via EBICS T, no SCA is required in some countries, while when the same client	The EBA clarifies that the SCA requirement in Article 97 PSD2 applies to all instances where the PSU 'accesses its payment account online', including 'when the information is requested through an account information service provider' (Articles 97(2)(a) and 97(4) PSD2), irrespective of the type of the access interface used for accessing the payment account online (i.e. irrespective of whether this is the ASPSP's customer interface, a dedicated interface, or a commercial interface).	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	wants to access the account information via a PSD2 API, it has to perform an SCA. These respondents were of the view that such commercial or 'premium APIs' that allow ongoing access to the account information without SCA are non-compliant with the PSD2 and the RTS and argued that the SCA rules should apply in the same way for all interfaces offered by ASPSPs, irrespective of the type of the access interface used for accessing the payment account information (i.e. irrespective of whether it is the customer interface, a dedicated interface or a commercial interface). These respondents asked the EBA to clarify that the exemption in the Article 10 applies to all accesses to the balance of payment accounts and payment transactions, and not just to the PSD2 dedicated interfaces.	Therefore, all access interfaces offered by ASPSPs that allow the PSU to access the PSU's payment account online should comply with the SCA requirement in PSD2, including any commercial interfaces provided by the ASPSP under a contractual arrangement with third parties that offer access to the PSU's payment account online (see also in this respect Q&A 6235). Accordingly, the exemption in Article 10 of the current RTS applies where the PSU is accessing online the payment account information specified in Article 10(1), directly or through an AISP, irrespective of the access interface used (i.e. irrespective of whether this is the ASPSP's customer interface, a dedicated interface or a commercial interface). Similarly, the mandatory exemption in Article 10a RTS applies where the PSU is accessing online the payment account information specified in Article 10a(1) through an AISP, irrespective of the type of the access interface used. The above is however without prejudice to the clarifications provided in response to comment 10 above regarding the implementation of the mandatory exemption in the customer interface for the purpose of the contingency mechanism in Article 33(4) RTS.	
20	One respondent argued that other fraud mitigation factors such as those mentioned in paragraph 35 of the CP may prove ineffective if AISPs do not share with the ASPSP the connectivity information (IP, navigator etc.) allowing the ASPSP to detect whether a connection is	The EBA notes that while the RTS does not explicitly require AISPs to share with the ASPSP connectivity information (such as https access logs, including IP address and device specification), the sharing of such information may be	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	risky or not. Said respondent argued that without the transmission of such information, the ASPSP cannot ensure its protection role.	useful for fraud prevention purposes, including to support effective transaction monitoring mechanisms as per Article 2 RTS. It is in both ASPSPs' and AISPs' interest in order to mitigate the risk of fraud to have in place arrangements in order to enable the sharing of fraud-related information, in compliance with Article 67 PSD2 and data protection requirements. In this respect, the EBA reiterates that both ASPSPs and AISPs are required to have in place security measures to mitigate the risk of fraud and detect unauthorised or fraudulent attempts to access the payment account data as explained in more detail in the response to comment 2 above. See also the response to comment 21 below.	
21	One respondent argued that TPPs should be able to instruct ASPSPs, at the discretion of the TPP, to apply SCA for individual customers if they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access, without impacting the rest of the SCA exemption.	As explained in the response to comment 2 above, where the AISP has reasons to suspect an attempt of unauthorised or fraudulent access, the AISP should take appropriate security measures to mitigate such risks. This may include for example (i) taking measures to verify the PSU' identity; (ii) requesting the application of SCA by the ASPSP (e.g. by requesting a new access token, where an access-token approach is used); and/or (iii) flagging to the ASPSP any suspicion of unauthorised or fraudulent access identified. In such latter case, this would represent a duly justified reason under Article 10a(3) for the ASPSP to apply SCA.	None
22	Several respondents were of the view that, if a mandatory exemption were to be introduced, there should be stricter requirements for	The EBA reiterates that in accordance with Article 67(2)(a) PSD2, AISPs can only access the payment account	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	AISPs to offer customers a clear and easy way to manage and revoke the consent given to the AISP. Other respondents suggested that the PSU should be allowed to revoke the consent given to the AISP via the ASPSP, particularly in cases when the AISP does not provide or communicate an easy process to revoke consent. In support of these proposals, some respondents mentioned that customers sometimes contact ASPSPs to ask how they can revoke a consent given to a TPP, because the TPP in question does not inform them clearly of this process. Also, another respondent argued that customers would have a higher level of control if they could check on the ASPSP's site all the TPPs to which they had previously given consent to access their account and withdraw the consent via the ASPSP. By contrast, other respondents were of the view that AISPs already provide PSUs with an easy way to stop access at any time, for example via the AISP's app or in other ways, and that this keeps the PSU in control.	information based on the PSU's explicit consent. It follows from this that where consent is revoked, the AISP is required to stop accessing the data, and would otherwise be in breach of law. The granting of the contractual consent given by the PSU to the AISP in accordance with Article 67(2)(a) and aspects related to its revocation are governed by the PSD2 and are outside the scope of the RTS and of this amendment. In this respect, the EBA recalls that the European Commission has clarified in its response to Q&A 4309 that 'it is only the PSU that can give consent to the provision of PIS and AIS services. It is consequently also the PSU that only has the right to withdraw the consent after it has been provided. The ASPSP cannot revoke the consent'. This being said, and separate from the issue of the revocation of the consent given to the TPP, as clarified in the response to comment 2 above, if the PSU has any concerns that a particular AISP might be accessing their account without consent, the PSU can also convey these concerns to their account provider which can decide accordingly to apply SCA to the next access request from the respective AISP in line with Article 10(3)(a), or deny access to the account in accordance with Article 68(5) PSD2, depending on the specific case and the ASPSP's risk assessment.	

No.	Summary of responses received	EBA analysis	Amendments to the proposals
23	One respondent noted that, while the EBA refers in the Consultation Paper to ASPSPs carrying out transaction monitoring, there is no explicit reference in the proposed new Article 10a to ASPSPs carrying out transaction monitoring in accordance with Article 2 RTS.	As explained in paragraph 35 of the CP, the EBA did not include a specific reference in Article 10a to ASPSPs carrying out transaction monitoring in accordance with Article 2 RTS because this requirement is not a condition to the application of the mandatory exemption, but it is a separate requirement that applies to all PSPs, irrespective of whether an exemption to SCA is used or not. The EBA is of the view that the application of the mandatory exemption should not be made conditional on the way in which ASPSPs have implemented the requirement in Article 2 RTS.	None
24	One respondent was of the view that the cross-reference in Article 10a(2)(b) to Article 10a(1)(b) could be interpreted to mean that no SCA renewal is required if the AISP is only accessing payment account balance information and sought clarification whether this was indeed the EBA's intention. The same question was also raised as regards the exemption in Article 10.	The exemption in Article 10 of the current RTS allows PSPs not to apply SCA when the PSU accesses, directly or through an AISP, the balance of the account and/or the last 90-day transaction history, provided that SCA was applied for the first access and is renewed at least every 90 days. The EBA clarifies that this 90-day timeline for the renewal of SCA starts to run from the last time SCA was applied for accessing either or both the balance of the account and/or the last 90-day transaction history. The above is also in line with previous clarifications provided by the EBA regarding the application of the exemption in Article 10 of the current RTS, including in paragraph 44 of the EBA Opinion on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04). Accordingly and for the avoidance of any doubt, the EBA has decided to clarify in the text of the RTS that the 180-day	Article 10(2)(b) of the RTS is amended as follows: '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'.

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		period in Articles 10(2)(b) and 10a(2)(b) starts to run from the last time SCA was applied for accessing online the information specified in paragraph 1 (i.e. either the balance of the account and/or the last 90-day transaction history).	Article 10a(2)(b) of the RTS is amended as follows: '(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'.
25	Several respondents sought clarifications as to what could be considered as 'objectively justified and duly evidenced reasons' to revert to SCA under Article 10a(3). Some respondents suggested clearly defining in the RTS what such reasons could be in order to avoid abusive blocking of TPPs, while other respondents were of the view that the ASPSP's right to apply	The EBA clarifies that Article 10a(3) is intended to capture all cases where the ASPSP has objective and justified reasons to suspect an attempt of unauthorised or fraudulent access to the payment account. This may include for example cases where the PSU notifies the ASPSP that their security credentials have been compromised, or that the PSU has reasons to suspect that a third party is accessing their account without their consent, as well as	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	SCA should not be unduly limited given the importance for ASPSPs to protect customers against fraud.	other cases where the ASPSP's monitoring mechanisms detect an elevated risk of unauthorised or fraudulent access. As clarified in the response to comment 21 above, this may also include cases where the AISP informs the ASPSP that it has reasons to suspect attempted unauthorised or fraudulent access for a particular access request. By contrast, as clarified in paragraph 32 of the CP, the sole fact that the ASPSP requires SCA each time customers directly access their payment account online is not a sufficiently justified reason under Article 10a(3) to not apply the mandatory exemption. To ensure that the provisions in Article 10a(3) are applied in a consistent manner and do not lead to abusive blocking of TPPs, Article 10a(3) requires ASPSPs to document and duly justify to their NCA upon request the reasons for applying SCA. Taking into account the multitude of scenarios that may arise in practice where there can be legitimate and justified grounds to suspect an attempt of unauthorised or fraudulent access, the EBA does not consider it necessary to be more prescriptive in Article 10a(3) as regards the reasons for applying SCA.	
26	Some respondents were of the view that the reference in paragraph 32 of the CP to 'transaction monitoring mechanism' is a wrong metric to use for account access by AISPs because the transaction monitoring	The EBA disagrees and notes that Article 2 RTS requires PSPs to have in place transaction monitoring mechanisms that enable them to detect unauthorised or fraudulent	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	in Article 2 RTS is primarily focused on unauthorised and fraudulent 'payment transactions' (rather than access). Some respondents suggested referring instead to 'credible intelligence, for example, from payment service user complaints, or other fraud-monitoring channels that indicate an elevated risk of unauthorised or fraudulent access to account data'.	payment transactions. While this article does not refer specifically to access to the payment account, unauthorised access to the account can lead to unauthorised or fraudulent payment transactions. Therefore, the ASPSPs' transaction monitoring mechanisms should also cover access to PSUs' payment accounts. Moreover, the EBA recalls that in line with the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), all PSPs are required to establish and implement policies and procedures to detect anomalous activities that may impact their information security and to respond to these events appropriately including, among others, monitoring transactions to detect misuse of access by third parties or other entities (see Section 3.4.5b of the guidelines).	
27	One respondent was of the view that Article 68(5) PSD2 provides a suitable mechanism for ASPSPs to block access to AISPs where there is a suspicion of fraudulent or unauthorised access, and that the proposed Article 10a(3) is redundant at best, and, at worst, risks limiting the utility of Article 10a.	The EBA disagrees and is of the view that the ability for ASPSPs to revert at any time to SCA where they have objective reasons to suspect an attempt of unauthorised or fraudulent access as per Article 10a(3) is an important safeguard to ensure that customers' data are protected. As explained in paragraph 33 of the CP, where an ASPSP has objective and justified reasons to suspect an attempt of unauthorised or fraudulent access, the ASPSP has the choice to apply SCA in accordance with Article 10a(3) or deny access to the account in accordance with Article 68(5)	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		PSD2, depending on the specific case and the ASPSP's risk assessment.	
28	One respondent sought clarifications on how the notification process in Article 10a(3) will operate, particularly regarding the burden of proof regarding the suspicion of fraud.	The burden of proof as regards the ASPSP's reasons for reverting to SCA in accordance with Article 10a(3) lies with the ASPSP. In line with Article 10a(3), the ASPSP should document and duly justify to its NCA, upon request, the reasons for applying SCA.	None
29	One respondent sought clarifications on who (the AISP or the NCA) should request that the ASPSP documents and justifies the reasons for applying SCA.	As clarified in Article 10a(3), the NCA can request the ASPSP to justify the reasons for reverting to SCA. AISPs, as well as PSUs, can approach the NCA where they consider that an ASPSP does not comply with the mandatory exemption.	None
30	One respondent suggested that, in order to avoid potential misuse by ASPSPs of the possibility in Article 10a(3) to revert to SCA, ASPSPs should be required in all cases to report to their NCA the reasons for reverting to SCA, and not only upon request. Also, another respondent suggested that in order to avoid abusive blocking of TPPs, the ability of ASPSPs to revert to SCA under Article 10a(3) should be further limited, e.g. only if duly notified, justified and accepted by the relevant NCA. Furthermore, a third respondent suggested that the EBA, together with NCAs, should ensure that the derogation to the new mandatory SCA exemption in Article 10a(3) is applied in a consistent and non-discriminatory manner by ASPSPs and is supported by the ASPSP's	The EBA is of the view that systematic reporting by ASPSPs of all the cases where they apply SCA on the basis of Article 10a(3), or a requirement for NCAs to periodically request and review all the cases where ASPSPs apply SCA on the basis of Article 10a(3) would impose a disproportionate burden on ASPSPs and NCAs. Furthermore, the EBA clarifies that the notification provided for in Article 10a(3) is always *ex post*, after SCA was applied, and that it would not be feasible to make the application of SCA conditional upon the prior notification and acceptance by the NCA. The NCA has discretion whether or not to request the ASPSP to justify the reasons for reverting to SCA on the basis of	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	documented rationale that is requested and reviewed by NCAs on a regular basis.	Article 10a(3). In supervising compliance with these requirements, NCAs may take into account complaints received from TPPs and PSUs.	
31	One respondent suggested that ASPSPs should be required to promptly notify AISPs when they seek to apply the derogation in Article 10a(3), at the same time they inform their competent authority. Also, another respondent suggested introducing transparency of the decisions taken.	The EBA is of the view that a requirement to notify the AISP at the same time as informing the NCA regarding the reasons for applying SCA would impose a disproportionate burden on ASPSPs. If an AISP considers that an ASPSP does not comply with the mandatory exemption, it can approach the NCA which can then ask the ASPSP to provide justification and documentation of the reasoning for applying SCA. As regards the suggestion to have transparency in the decisions taken, the respondent does not clarify to what decisions it refers. If this refers to the NCA's assessment of the reasons provided by the ASPSP for applying SCA, the EBA does not consider that further specification in this respect in the RTS is needed and notes that the transparency of the decisions taken by NCAs in fulfilment of their supervisory duties is a matter of national law. If this refers to the ASPSP's assessment and decision to apply SCA on the basis of Article 10a(3), the EBA clarifies that ASPSPs are not required to justify to the AISP the reasons for applying SCA – in this respect, see the response to comment 30 above .	None
32	Some respondents commented that some AIS-use cases only require one-off access to the account information, for example in order to	The EBA is of the view that the current legal framework already includes sufficient safeguards to ensure that AISPs	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	perform a one-off credit affordability assessment as part of a lending decision, and that in such cases, the AISP should not actively continue to access the customer data for the full 180 days. These respondents suggested that the EBA should consider the safeguards in place to ensure that AISPs comply with the principle of data minimisation, and only request the data that they need for their customer proposition.	only access the data they need for the provision of their services based on the customer's explicit consent. In particular, the EBA reiterates that, in accordance with the PSD2, AISPs can provide their services only where based on the PSU's explicit consent (Article 67(2)(a) PSD2), and are forbidden to use, access or store any data for purposes other than for performing the AIS explicitly requested by the PSU in accordance with data protection rules (Article 67(2)(f) PSD2). In addition, Article 36(3) RTS requires AISPs to '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'. Furthermore, the EBA recalls that AISPs are also subject to the GDPR requirements, including the requirements in Article 5(1)(c) GDPR on data minimisation and the obligations in Article 25 of GDPR to apply data protection by design and by default.	
33	Some respondents suggested that the payment transaction history that can be retrieved using the SCA exemption should be extended from the last 90-day transaction data to the last 180- or 365-day transition history. These respondents argued that 90 days is too short a period for most AIS-use cases to present to the PSU the AISP solution as a useful and effective solution and that extending this period to 12 months would be preferable, given that 12 months of data are usually made available to the PSU in the ASPSP's direct customer channels.	The EBA does not consider that there are compelling arguments to extend the payment transaction history that can be accessed using the exemption to SCA in Articles 10 or 10a. AISPs can already retrieve the full transaction history with the application of SCA and rely on the exemption in the RTS for retrieving the last 90-day transaction history.	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	A few respondents suggested removing altogether any limitation of the transaction history that can be retrieved using the exemption.	Furthermore, the limited scope of the payment account data that can be accessed using the exemption is one of the elements that contribute to ensuring that the exemption is compatible with the level of risk involved, in line with Article 98(3)(a) PSD2.	
34	One respondent suggested amending Article 36(5)(b) RTS so that the four-times-per-day counter is applied as a separate counter for each account information request type (e.g. balance requests and transaction list requests) and for each payment account.	These aspects are not related to the application of the SCA exemption for AIS and go beyond the scope of this consultation. Q&A 4210 provides clarifications on the application of the four-times-per-day counter in Article 36(5)(b).	None
35	One respondent was of the view that using two elements categorised as inherence (e.g. biometric technologies that combine face and voice recognition) should be enough to meet the SCA requirement and asked the EBA to reconsider its opinion that the two elements of SCA should belong to different categories.	These aspects are not related to the application of the SCA exemption for AIS and go beyond the scope of this consultation. Paragraph 33 of the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04) and Q&A 5619 provide further clarifications in this respect.	None
36	One respondent representing several manufacturers and operators of charging points for electric vehicles suggested introducing into the RTS an additional exemption from SCA for payments at charging stations for electric vehicles. These respondents argued that if, in the implementation of the SCA requirement in PSD2, a PIN pad is required to be installed on the charging station, this will have considerable consequences for the costs and installation space, especially of alternating current (AC) charging stations.	These aspects are not related to the application of the SCA exemption for AIS and go beyond the scope of this consultation. Q&A 5224 provides clarity on the application of the current exemptions in the RTS to transactions at unattended terminals for the payment of a parking fee that includes electric charging.	None
Q2. Do you have any comments on the proposal to extend the timeline for the renewal of SCA to 180 days?			

No.	Summary of responses received	EBA analysis	Amendments to the proposals
37	Some respondents were of the view that the proposed 180-day period for the renewal of SCA could increase the risk of fraud and that the current 90-day period in Article 10 RTS should be maintained. These respondents argued that the current 90-day timeline ensures a good balance between security and a smooth customer journey, and that extending the timeline for the renewal of SCA could increase the risk that if a customer doesn't want to use the services of an AISP anymore and is not able to reach the AISP to withdraw consent, or the AISP doesn't act on it, the AISP will still have access to the account data for the remaining 180-day period. Other respondents supported the proposed 180-day period for the renewal of SCA and were of the view that it strikes a good balance between good user experience and a high level of security. A third group of respondents were of the view that the proposed 180-day period is too short and suggested instead to extend it to 1 year or more (a few respondents suggested extending it to 2 years). These respondents argued that a 1-year timeline: - would be a suitable time frame given the low risk of fraud risk associated with AIS and the safeguards that the EBA is proposing to apply to the new exemption; - would allow AISPs to establish a customer base and build up customer loyalty before the first SCA is required; - may be particularly beneficial for some AIS-use cases, such as cloud accounting services.	Having assessed the arguments presented by these respondents, the EBA has decided to retain the 180-day period for the renewal of SCA proposed in the CP. In the EBA's view, the renewal of SCA every 180 days, combined with the possibility for the ASPSP to revert to SCA at any time if it has justified reasons to suspect attempt unauthorised or fraudulent access and the other safeguards detailed in the response to comment 2 above, strike a good balance between the PSD2 objectives of ensuring security and the innovation and competition enhancing objectives of PSD2, in line with Article 98(3)(a) PSD2. Regarding the suggestion made by some respondents to altogether remove the requirement to renew SCA, as explained in the response to comment 13 above, this would not be a feasible option under the PSD2. This is because Articles 97(1)(a) and 97(4) of PSD2 are clear that SCA is required when the PSU accesses its account information online, including 'when the information is requested through an account information service provider'. Therefore, such changes cannot be brought about by amending the RTS, and would require a change of the PSD2, which is not within the EBA's powers to bring about.	None.

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	These respondents also emphasised that PSUs can at any time stop access to the data directly with the AISPs, and that this keeps the PSU in control. Finally, a fourth group of respondents were of the view that the requirement to renew SCA should be removed altogether (see in this respect comment 13 above).		
38	Some respondents suggested that instead of mandating SCA renewal at a predetermined frequency, customers should be allowed to choose if they want SCA to be applied for a specific AISP and decide, on an individual basis, whether or not to enable an exemption and the timeline for the renewal of SCA.	As explained in the response to comment 12 above, when developing the draft amending RTS, the EBA has also considered the possibility of allowing the PSU to decide how often SCA should be applied when using the services of an AISP. However, the EBA discarded such an approach because 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, based on the criteria in Article 98(3) PSD2, and cannot be defined based on individual choices of each PSU. Furthermore, such an approach may go against the PSD2 objective of enhancing security if the time period chosen by the PSU for the renewal of SCA is not compatible with the level of risk involved. Moreover, this could lead to very divergent practices in the application of SCA that would generate an unproportionate burden for all PSPs in applying SCA and would further exacerbate the issues faced by AISPs. For these reasons, the EBA has discarded this option.	None
39	One respondent was of the view that if a customer performs any other authentication action when using the services of the same TPP, for example, to initiate a payment, the frequency for the renewal of SCA	The EBA clarifies that the 180-day period in Article 10a is specific to each AISP and that initiating a payment using the services of the same TPP (that is authorised to provide both	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	when using the AIS offered by the same TPP could be extended beyond 180 days.	AIS and PIS) does not restart the 180-day counter. This is in line with the clarifications provided in paragraph 44 of the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04) regarding the calculation of the current 90-day period in Article 10 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 1 month before such changes are required to be implemented?			
40	Some TPPs supported the proposed 1-month period for making available to TPPs the changes to the technical specifications of ASPSPs' interfaces ahead of their implementation and were of the view that this timeline would be feasible from their perspective. Some of these TPPs added that they would not object to this compressed timeline if the overall implementation timeline for ASPSPs is also reduced from 6 to 3 months. By contrast, other TPPs were of the view that a 1-month period would be insufficient and would not allow them to understand the technical specifications of all the ASPSPs to which they are connected, discuss these if necessary with the ASPSPs, and make the necessary changes to the TPP's systems. These TPPs asked to retain the minimum 3-month period in Article 30(4) RTS for making available to TPPs the changes to the technical specifications of ASPSPs' interfaces ahead of their implementation.	Having assessed the arguments presented by these respondents, the EBA has decided to extend the period for making available to TPPs the changes to the technical specifications of ASPSPs' interfaces from 1 to 2 months ahead of their implementation. This aims to ensure that TPPs will have sufficient time to make any necessary changes to their systems ahead of the implementation of the respective changes by ASPSPs. The EBA understands that the technical changes that AISPs would need to make to their systems are limited particularly in cases where the ASPSP uses an access-token approach for granting access to TPPs to the account information, and that therefore a 2-month period should be sufficient for AISPs to implement the necessary changes in their systems.	Article 2 of the draft amending RTS is amended as follows: '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

No.	Summary of responses received	EBA analysis	Amendments to the proposals
			the changes made to the technical specifications of their interfaces in order to comply with this Regulation not less than ~~one~~ **2** month**s** before such changes are implemented'.
41	One respondent suggested that, in order to support compliance with Article 2 of the draft amending RTS, the EBA together with NCAs should create a central database that can be accessed by TPPs to view ASPSPs' technical specifications.	The EBA is of the view that the industry is better placed to create such databases and encourages industry participants to publish information on ASPSPs' testing facilities (including weblinks to ASPSPs' developer portals) in order to support the testing by AISPs.	None
42	One respondent suggested that the EBA should work together with NCAs to ensure that ASPSPs make available the necessary integration and testing resources to facilitate AISPs' transition to the revised ASPSPs interfaces within the 1-month timeline.	The supervision of ASPSPs' compliance with the amending RTS, including with the period specified in Article 2 of the draft amending RTS for making available to TPPs the changes to ASPSPs' interfaces ahead of their implementation, will be part of the NCAs' general supervisory duties under the RTS.	None
43	Some respondents, in particular TPPs, were of the view that the proposed 6-month implementation period is too long and suggested	Having assessed the arguments presented by these respondents, the EBA has decided to extend the implementation period from 6 to 7 months after the publication of the amending RTS in the Official Journal of	Article 3 paragraph 2 of the draft amending RTS is

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	reducing it to 3 months given the urgency of addressing the issues at stake for AISPs. By contrast, other respondents, in particular ASPSPs, were of the view that a 6-month implementation period would be too short for ASPSPs to implement the required changes in their systems and suggested extending it to 9 months or 1 year. Some of these ASPSPs noted that they would prefer a 1-year timeline not so much because of the complexity of the changes, but rather due to the need to accommodate technology investment decision-making timeframes and emphasised that an estimated application date in Q4 2022 would be too short given that budgets for the year 2022 are already closed. Also, some ASPSPs argued that a 9-month to 1-year timeline would be a more realistic approach and would increase the chances of having a smooth transition to the new requirements. Finally, one respondent was of the view that the implementation of the mandatory exemption would require a longer implementation period especially for ASPSPs that do not currently support the exemption in Article 10 RTS.	the EU as a Commission Delegated Regulation. This takes into account the extension of the timeline for making available to TPPs the changes to the technical specifications of ASPSPs' interfaces from 1 to 2 months ahead of the implementation of those changes, as explained in the response to comment 40 above. Given the targeted nature of the amendments to the RTS, the EBA is of the view that this should give sufficient time to both ASPSPs and AISPs to implement the necessary changes in their systems, make any necessary amendments to the terms and conditions with the PSU in line with Article 54 of PSD2 and communicate and explain these changes to PSUs before the application date of the amending RTS. Finally, with regard to the concerns raised by some ASPSPs regarding the estimated application date of the amending RTS potentially falling in Q42022, the EBA notes that the application date of the draft amending RTS will depend on the legislative process for its adoption by the EU Commission and the EU Parliament and Council, which is not within the EBA's control.	amended as follows: '2. This Regulation shall apply from [OJ please add date corresponding to ~~6 (six)~~ **7 (seven)** months after entry into force date].'
44	Several respondents sought clarifications on whether the existing 90-day SCA access tokens issued to AISPs before the application date of the amending RTS will remain valid until their expiration at the end of the 90-day period and whether only the access tokens issued after the application date of the amending RTS must comply with the 180-day rule.	The EBA clarifies that starting with the application date of the amending RTS, ASPSPs should allow AISPs to access the payment account information without SCA for a period of 180 days, subject to the application of SCA for this initial access request and the other conditions for the application of the exemption in Article 10a being met. This means that,	A new paragraph (3) is introduced in Article 3 of the draft amending RTS as follows:

No.	Summary of responses received	EBA analysis	Amendments to the proposals
	In this respect, one respondent indicated that the length of the access token that is provided to the AISP (to enable it to access the data without SCA) is hard-coded into the token upon issuance and that there will be a hard switchover to the new token length of 180 days. This would mean that during a transition period (of approx. 90 days) both tokens (with a 90-day and 180-day validity) will be used, depending on when the token was issued (i.e. before or after the switchover to the new 180-day tokens). The respondent suggested that the EBA should explicitly address this point to drive consistency across the market.	for the particular case where an access-token approach is used for granting access to AISPs to the payment account, any new access token issued on or after the application date of the amending RTS should comply with the mandatory exemption in Article 10a. Where ASPSPs have applied the exemption in Article 10 RTS prior to the application date of the amending RTS, they can continue applying that exemption and allow access to AISPs without SCA up to 90 days from the last time SCA was applied. This is however without prejudice to the application of the mandatory exemption in Article 10a for new access requests received through an AISP starting with the application date of the amending RTS, as explained above. This has been clarified in the new Article 3(3) of the draft amending RTS.	'3. Payment service providers that applied the exemption in Article 10 of Delegated Regulation (EU) 2018/389 prior to the application date in paragraph 2 shall be allowed to continue applying that exemption up to 90 days from the last time SCA was applied'.
45	One respondent sought clarifications as to whether, on the application date of the amending RTS, the 180-day period for the renewal of SCA will continue to be calculated from the time SCA was last applied, or whether the 'clock' gets reset so that the 180 days begins from the application date of the amending RTS.	As clarified in Article 10a(2)(b), the 180-day period for the renewal of SCA is calculated from the last time SCA was applied for accessing the account information through the AISP. Where an access-token approach is used for granting access to AISPs to the payment account information, SCA will be required for the initial access request and the issuance of the token. This means that for access requests received from AISPs on or after the application date of the draft amending RTS requesting the issuance of a new 180-day	None

No.	Summary of responses received	EBA analysis	Amendments to the proposals
		token, SCA will be applied for the issuance of the token, irrespective of the last time when SCA was applied for accessing the account information through the respective AISP (see also the response to comment 44 above). For subsequent access requests, the 180-day period in Article 10a(2)(b) for the renewal of SCA will be calculated from the last time SCA was applied for accessing the account information through the AISP.	
46	One respondent was of the view that if ASPSPs were to implement changes to the technical specifications of their interfaces at different times during the 6-month implementation period, this could pose challenges for TPPs in relation to updating their terms and conditions. For example, if ASPSPs are operating on the basis of a mixture of 90-day and 180-day SCA renewal during the implementation period, either the PSU journey of TPPs will have to be dynamic (reacting to each ASPSP with a different experience/ terms and conditions), or less specific/precise to cover all options (e.g. 90- to 180-day SCA renewal depending on the maximum term that each ASPSP supports).	The EBA clarifies that until the application date of the amending RTS specified in Article 3(2) of the draft amending RTS, the requirements set in Article 10 of the current RTS continue to apply, including the 90-day limit for the renewal of SCA. This means that requiring SCA renewal every 180 days earlier than the application date of the amending RTS would not be compliant with the RTS.	None
47	One respondent sought clarification on whether it is possible to maintain the current 90-day timeline for the renewal of SCA during the proposed 6-month implementation period.	As explained in the response to comment 46 above, until the application date of the amending RTS as specified in Article 3(2) of the draft amending RTS, the requirements set in Article 10 of the current RTS continue to apply, including the 90-day period for the renewal of SCA.	None