POSITION PAPER

**ESBG response to the EBA Consultation Paper on the amendment of the RTS on SCA&CSC in relation to the 90-day exemption for account access**

ESBG (European Savings and Retail Banking Group)

Rue Marie-Thérèse, 11 - B-1000 Brussels

ESBG Transparency Register ID 8765978796-80

**November 2021**

ESBG

**ESBG Response to the European Banking Authority Consultation Paper Consultation Paper on the amendment of its RTS on SCA&CSC in relation to the 90-day exemption for account access**

The European Savings and Retail Banking Group (ESBG) welcomes the opportunity to respond to this public consultation from the European Banking Authority on the amendment of its Regulatory Technical Standards (RTS) on Strong Customer Authentication and Secure Communication (SCA&CSC) under the Payment Services Directive (PSD2) with regard to 90-day exemption from SCA for account access.

As a general remark, ESBG and its members strongly disagree with the EBA's claim that ASPSPs failed to provide user-friendly SCA methods so that the application of SCA in most cases causes friction in the customer journey. The RTS on SCA & CSC establish the requirements to be complied with by payment service providers (PSPs) for the purpose of implementing security measures which enable them to apply the procedure of strong customer authentication in accordance with Article 97 PSD2. The RTS also provide for exemptions from the application of the security requirements of SCA, subject to specified and limited conditions, inter alia based on the level of risk. Therefore, the decision to exempt the application of SCA within the limits of the regulation is solely based on the risk-assessment of the ASPSP, that is ultimately responsible vis-à-vis its customers. It follows that the proposed mandatory exemption is in contradiction to Article 1 Delegated Regulation (EU) 2018/389. Additionally, Article 97(1) PSD2 stipulates that PSPs shall apply SCA in certain situations and Article 98(1) PSD2 gives the EBA the mandate to exemptions from the application of SCA. This however does not give the EBA the mandate to make the exemption mandatory as that would rather represent the annulment of Article 97 SCA requirements. Further, a mandatory exemption to SCA would severely violate the principle of equivalence of treatment. This means ASPSPs would be prevented from the application of SCA when PSUs access through AISPs although they require SCA every time the PSUs is accessing their account information directly. Additionally, due to technical limitations, ASPSP can comply with the mandatory exemption in the dedicated interfaces only, while changes cannot be made in the alternative customer interfaces. It follows that this amendment proposed by the EBA is not technology neutral.

ESBG and its Members believe there is no material evidence identifying a need for the proposed change. The RTS on SCA & CSC have been in force for only two years and it took almost a year for ASPSPs to initiate aggregation activity in the dedicated interface and use of 90-day exemption. For that reason, an exhaustive analysis would be necessary as a first step. Said analysis must also evaluate if such change could impact the level of consumer protection and assess whether the proposal would ensure trust in all types of PSP is maintained.

As to the suggested 6-month implementation timeline, ESBG and its members are of the view this proposal does not consider that many ASPSPs have already fixed their implementation plans for the coming year, making it difficult to accommodate additional requirements that have to be implemented in 2022.

**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?**

ESBG and its members think it is too early to assess said proposal, especially as there is no material evidence identifying a need for the proposed change. The RTS on SCA & CSC have been in force for only two years and it took almost a year for ASPSP to initiate aggregation activity in the dedicated interface and use of 90-day exemption. For that reason, ESBG and its members believe an exhaustive analysis is necessary as a first step.

Inter alia, it must be properly evaluated if such change could impact the level of consumer protection and assess whether the proposal would ensure trust for open payments – for all types of PSP – is maintained. This has also not been raised as a problem by the PSUs of our members. These requirements must be correctly calibrated, otherwise they can have a negative effect on customer trust in the Open Payments industry.

Additionally, if there is a real and pressing need it cannot be ruled out that it would be more suitable to let the payment service user decide about enabling an exemption or not on an individual basis if this is legally possible. Measures taken should increase the confidence and trust in all PSPs in the value chain.

As such, ESBG and its members firmly oppose the approach taken with the suggested amendment. The obligation and responsibility to perform SCA lies solely on the ASPSP (Article 97 PSD2); indeed, it is the ASPSP that issues the personalised security credentials. On the one hand, ASPSPs cannot rely on the AISPs to conduct SCA on the ASPSP's behalf; on the other hand, ASPSPs cannot be forced to delegate SCA (as also confirmed by para 19 and 22 of the Consultation Paper). Therefore, we would welcome a clear guidance confirming the unambiguous responsibility of ASPSP as laid down in PSD2.

The RTS on SCA & CSC establish the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to apply the procedure of strong customer authentication in accordance with Article 97 PSD2. The RTS also provide for exemptions from the application of the security requirements of SCA, subject to specified and limited conditions, inter alia based on the level of risk. Therefore, the decision to exempt the application of strong customer authentication within the limits of the regulation is solely based on the risk-assessment of the ASPSP, who is ultimately responsible vis-à-vis its customers. It follows that the proposed mandatory exemption is in contradiction to Article 1 Delegated Regulation (EU) 2018/389.

Further, Article 97(1) PSD2 stipulates that PSP shall apply strong customer authentication in certain situations and 98(1) gives the EBA the mandate to exemptions from the application of SCA. This however does not give the EBA the mandate to make the exemption mandatory as a mandatory exemption is not an exemption but an intrusion of Article 97 SCA requirements; going against the mandate given to the EBA by the regulating institutions of the European

Union. This should instead be a topic for a future discussion in the upcoming PSD2 review.

One of the major goals of PSD2 was to improve the security of online banking. This is ensured via SCA and via the principle that the PSU themselves are controlling the access of third-party services to their payment account(s) at any time. The EBA's proposals could give the impression that these safeguards are to be eroded primarily for the benefit of one of the service providers regulated by PSD2. This is because the new exceptions are mainly in favor of account information services and EBA proposes to expand those significantly, without explaining apparently whether and how this is still compatible with the original approach of PSD2. Rather, there is a danger that a spiral for the extension of exemptions will be set in motion from time to time.

A mandatory exemption to SCA would severely violate the principle of equivalence of treatment. ASPSPs would be prevented from the application of SCA when PSUs access through AISPs although they require SCA every time the PSUs is accessing their account information directly. Additionally, due to technical limitations, ASPSP can comply with the mandatory exemption in the dedicated interfaces only, while changes cannot be made in the alternative customer interfaces. It follows that this amendment proposed by the EBA is not technology neutral. Additionally, it would be technically difficult, if not impossible, to implement the mandatory exemption without severely lowering the level of customer protection.

In case that ASPSPs have decided to apply SCA every time the user accesses his account directly it has to be considered that fraudsters will be able to undermine the security barriers of ASPSPs by using AISPs for getting access to user accounts where the security barriers are lower. Furthermore, it must be taken into account that the proposed amendment has serious impact on security considerations of ASPSPs. ASPSPs are hindered in their own risk assessment to provide a higher level of security.

On a separate note, we strongly disagree with the EBA's claim that ASPSPs failed to provide user-friendly SCA methods so that the application of SCA in most cases causes friction in the customer journey. Since 2016 a lot of ASPSPs have developed user-friendly SCA methods making use of possession and inherence elements as proposed in the RTS, rather than solely relying on knowledge factors like static passwords or authentication codes that have to be typed in by the user. For many PSU today SCA simply means tapping on a smartphone (i.e., fingerprints) or entering a code. A mandatory exemption when the PSU accesses through an AISP may lead to even more conflicting situations and irritations on the PSUs, since this will lead to different experiences regarding the application of SCA depending on whether they are accessing their payment account directly or not.

We also fear that a mandatory exemption from SCA would increase customer integrity risks. In each situation that a user downloads a token on a device, any other individual using that same device will be able to access the financial data

of that user, as the ASPSP cannot determine who is actually using the device. This will make the PSU more dependent on the security levels of the technical device that it uses, which is again not in control of the ASPSP. Not all devices have the same SCA level such as a digital ID-scheme or in the future a European ID Scheme.

A reduced level of security increases the risk of unauthorised access to data. For the user it might be of interest to have the choice of using a SCA exemption or not. In relation to the criteria in Article 98(3) PSD2, setting a mandatory exemption would require the EBA to make the ex-ante assumption that the risk-level will always and in all AIS situations be on a low level, contradicting the requirements set in RTS Article 1(b) and hence not fulfilling the requirements in Article 98(3) PSD2:

a) the level of risk involved in the service provided;
b) the amount, the recurrence of the transaction, or both;
c) the payment channel used for the execution of the transaction.

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

In the final report on the draft RTS on SCA&CSC (EBA/RTS/2017/02), the EBA considered the 90 days to be an appropriate balance. We lack a substantial analysis on the real need to extent the timeline, and how such extension could impact the level of consumer integrity protection. As of today, we do not see any need for the extension of the timeline for SCA renewal, as we do not have evidence that the current 90-day period is an obstacle for product offerings or a reason for customer complaints. Therefore, we encourage the EBA to further analyse the matter as part of the upcoming review of PSD2. A further extension to 180 days could have the potential to reduce PSUs' sovereignty over their data and increase risks. Indeed, the renewal of SCA acts as both a security mechanism as well as a warning and information function. A period of 6 months without renewal of SCA or direct action of the PSU for third party data retrieval does not meet these requirements and will be at the disadvantage of PSUs. It could lead to a greater loss of confidence to the detriment of all market players.

Overall, we strongly suggest that any extension be reconsidered in a few years' time, once PSPs, PSUs, and authorities have gained more experience with customer needs, security concerns, and related data protection aspects to evaluate the impact more thoroughly.

Nevertheless, should the EBA decide to maintain the change to extend the extension from 90 to 180-days, then the same extension for the renewal of SCA should apply both for the access through an AISP and when customers access directly the account information, to ensure a level playing field for all PSPs.

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

| |
|---|
| The suggested 6-month implementation timeline and estimated take effect from Q4 2022 onwards does not consider that many ASPSPs have already fixed their implementation plans for the coming year, making it difficult to accommodate additional requirements that have to be implemented in 2022. Therefore, a 12-month implementation timeline with an estimated entry into force in 2023 would be more suitable. |

## About ESBG (European Savings and Retail Banking Group)

ESBG is an association that represents the locally focused European banking sector, helping savings and retail banks in 18 European countries strengthen their unique approach that focuses on providing service to local communities and boosting SMEs. An advocate for a proportionate approach to banking rules, ESBG unites at EU level some 885 banks, which together employ 656,000 people driven to innovate at 48,900 outlets. ESBG members have total assets of €5.3 trillion, provide €1 trillion billion in corporate loans, including SMEs, and serve 150 million Europeans seeking retail banking services. ESBG members are committed to further unleash the promise of sustainable, responsible 21st century banking.

European Savings and Retail Banking Group – aisbl
Rue Marie-Thérèse, 11 ▪ B-1000 Brussels ▪ Tel: +32 2 211 11 11 ▪ Fax : +32 2 211 11 99
Info@wsbi-esbg.org ▪ www.wsbi-esbg.org

Published by ESBG. November 2021.