EBF Response to European Banking Authority's Consultation on amending RTS on SCA and CSC under PSD2 (EBA/CP/2021/32)

25 November 2021

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?

We welcome the opportunity to comment on this consultation.

The implementation of PSD2 has been a rather complicated process for ASPSPs and the whole market. Some of this complexity is due to uncertainties on what actually constitutes the regulatory perimeter and the multiple clarifications issued by authorities that have moved the goalpost in terms of implementation. The EBF considers that it is important for the market to have clarity and certainty that this amendment will be the only aspect eventually to be amended in the legal framework before the formal review of PSD2. Having said this, we find the timing of this proposal difficult in view of the upcoming PSD2 review. It is highly likely that this topic will be part of the PSD2 review and it could be that a completely different assessment of this exemption would be made and that a completely different implementation would be required under a possible PSD3. It is not justified in our view that ASPSPs should be obliged to make the required changes and carry their implementation costs, only to be potentially applied for a short time.

We acknowledge that the issue of 90-days SCA renewal has widely been raised by AISPs as a particularly problematic aspect of PSD2 implementation and the need of the EBA to explore possible solutions. However, as it is important to balance different market views, we are of the view that a **mandatory exemption is not appropriate**. The exemption should remain voluntary in order to allow ASPSPs to address any potential increase in risk of fraud as per bank risk appetite, whilst also ensuring flexible legislation that does not stifle innovation and cause unnecessary friction in the customer experience. A mandatory exemption would neither allow banks to apply risk-based approach, to carry out an adequate risk and fraud-management, nor to apply the appropriate protection to their customers. The RTS should set a standard, high level of customer protection (SCA) and then carve out exemptions where banks can implement at a discretionary basis. Also, already as it stands, the **liabilities and risks** in the PSD2 are not fairly balanced between ASPSP and PISP/AISP and the proposed amendments to Article 10 would worsen this unbalance as the liability would still sit with the ASPSPs. The proposed amendments would reduce the discretionary capability of ASPSPs on their authentication processes, and should this amendment be adopted, it would be important to ensure

European Banking Federation aisbl

Brussels / Avenue des Arts 56, 1000 Brussels, Belgium / +32 2 508 3711 / info@ebf.eu
Frankfurt / Weißfrauenstraße 12-16, 60311 Frankfurt, Germany
EU Transparency Register / ID number: 4722660838-23

www.ebf.eu

that any additional risk that could emerge by this obligation were borne by the AISPs, being the beneficiaries of the proposed amendment. The entity that benefits from the advantages of SCA exemption should also have the burden of proof and manage the relationship with the customer in case of complaints (as it is the case by the way also in the cards world already now).

Additionally, it is not the voluntary nature of the exemption that has led to divergent practices across the EU in its application, but the competitive nature of the provision of the payment services in Europe, and the different proposals carried out by PSPs, this in terms of customer experience, risk appetite, and many other factors.

Although we are of course aware of the complaints by AISP, we believe that there is not a sufficient **impact assessment and substantial justification** for proposing this amendment. In the final report on draft RTS on SCA and CSC, the EBA stated the EBA considered that the 90 days to be an appropriate balance. We lack a substantial analysis on why this is no longer the case, what is the real need to amend the RTS and what the impact of such a change would have. We also question the argument made by AISPs that the decline in AISP customers at 90 days would be due to the SCA renewal process as it may very well be that AISP customers simply do not wish to continue with the AISP services.

It must also be evaluated if the proposed changes could impact the level of **consumer protection and security**. We are concerned of a negative effect on customer trust in the 'open payments' industry. Measures taken should increase the confidence and trust in all PSPs in the value chain. For a mandatory exemption, there is an increased customer integrity risk. 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 uses the device. This will make the PSU more dependent on the security levels of the technical device that it uses, which is not in control of the ASPSP and which may not have the same level of security than that provided by the application of SCA.

In terms of risk of fraud, we consider that it is important to balance the objectives of convenience with **fraud prevention and security**, which are also key objectives of PSD2. It should be considered that a mandatory SCA exemption and an extension of the SCA validity to 180 days could indirectly increase the risk of fraud, as fraudsters could repeatedly have unauthorised access during the longer timeframe of 180 days, obtaining more customer information more easily than currently. Even if access to account information could at first hand be considered less risky than e.g. payment initiation, it should not be forgotten that an increasing number of fraud is related to fraudsters gaining access to detailed data and information about a customer. Most scams committed are initiated by sophisticated social engineering techniques making use of all customers' data available, whether they are consumers or employees of SMEs or big corporations. Payments-related data in hands of criminals makes it very easy for them to impersonate the bank in front of the customer that will rely on them just because of the nature of the concrete piece of information they possess.

Further, it should be well noted that the proposed suggested exemption will only benefit one type of PSP i.e. the AISP. This would deviate from the principle of "same activity, same risk, same rules". A mandatory exemption to SCA would **undermine the principle of equivalence of treatment and level playing field between PSPs**. ASPSPs would be prevented from the application of SCA when PSUs access through AISPs although many require SCA every time the PSUs is accessing their account information directly. If introduced, the mandatory exemption should only be applied when the ASPSP also offers this exemption in the direct customer interface which would be in line with Article 67(3)(b) of PSD2 i.e. that the ASPSP should treat AISP without any discrimination.

We would encourage the EBA to consider what safeguarding is in place to ensure that AISPs adhere to the principles of data minimisation, and only request the data that they require for their customer proposition. For example, a number of AISP use cases would suggest that data is only required once, for a specific decision (e.g. to perform a one-off credit affordability assessment as part of a lending decision). For this type of use case, AISPs should not actively continue accessing the customer data for the full 180-days (unless they have a clear reason for doing this and have explicit consent from the customer). If a mandatory exemption were to be adopted, it should be complemented with the need to ensure that customers might be able to revoke previous consent given to the AISPs. There is evidence that customers approach the ASPSPs to ask for the cancelation of the service, that is, requesting to stop the exchange of information with an AISPs, for instance for a for a single-access AISP service such as described above.

As for the text of the new Article 10a *"Access to the payment account information through an account information service provider",* the experience gained in the application of the PSD2 and the RTS has shown that unprecise expressions do not help the market to implement harmonised solutions across the EU. It is the case of "objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account" in the proposed Article 10a(3). In case the SCA exemption was to be made mandatory, we would prefer **detailed legal requirements to be applied in order to revert to SCA**, which would avoid complaints from the AISPs and over-reporting to the NCAs. In this context we would also like to express our concern that in the proposed new Article 10a there is no explicit reference to ASPSP carrying out transaction monitoring in accordance with Art 2. The EBA refers in the consultation paper to ASPSP carrying out transaction monitoring but this is omitted from the text. Therefore, for Article 10, the ASPSP can require SCA based upon its assessment of Article 2 transaction monitoring. For Article 10(a), the ASPSP will be required to allow AISP access to customer accounts for at least 180 days unless it can document and justify to its national regulator (if requested) why there was an objectively justified and duly evidenced reason why the access to the account would be unauthorised and fraudulent. It should also be noted that the ASPSP will be required to evidence why account access would be unauthorised or fraudulent before requiring SCA which would be a very high burden to discharge.

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

In terms of the RTS amendments proposed, it is more important to re-consider the mandatory nature of the exemption than the number of days of the exemption, as developed above. However, we do believe that 180 days is the maximum to which the timeline should be extended. In addition to the concerns raised above regarding security and fraud, we would like to highlight that the extension to 180 days could have some other undesired effects. For instance, in case of mistakes in managing the revocation of the consent by the customer, the AISP will automatically access the accounts information as long as the 180 days deadline expires. The possibility that this could occur is now extended within a longer period of time and this increases issues on the third party's access to payment account from the security and privacy perspectives.

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?

It is important to note that the implementation period needs to consider that **most of the implementation burden is on the ASPSP side.** Furthermore, budgets for the year 2022 are already closed and budgeting these changes for 2022 would be very difficult, therefore implementation in 2023 would be much preferrable. For implementing the mandatory exemption for the case when the information is accessed through an AISP a longer implementation period of one year would be needed. For a solution consisting only of an extension to 180 days for renewing SCA 6-months after publication in the official journal could be enough.

We also think it would be necessary to clarify in the amended RTS that the existing 90-SCA grants given before the date of entry into force of the amended RTS remain valid until end of the 90-day period, so during the first three months after the effective date these 90 days grants will expire and upon such expiry the 180 days shall apply.