EBA/CP/2021/32

BSG 2021 073

1 December 2021

BANKING STAKEHOLDER GROUP

EBA Consultation Paper on Draft Regulatory Technical Standards amending the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

On 28 October 2021, the EBA issued a consultation on Draft Regulatory Technical Standards amending the Commission Delegated Regulation (EU) 2018/389 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

The revised Payment Services Directive (EU) 2015/2366 (PSD2) has introduced the requirement for payment service providers (PSPs) to apply strong customer authentication (SCA) each time a payment service user (PSU) accesses its payment account online. At the same time, the PSD2 mandated the EBA to develop regulatory technical standards (RTS) specifying, amongst others, the requirements of SCA and the exemptions to SCA.

In particular, Article 10 of the RTS provides an exemption from the application of SCA when the customer accesses limited payment account information, provided that SCA is applied for the first access and at least every 90 days after that.

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

The EBA is now proposing to make this exemption mandatory for ASPSPs, subject to certain safeguards and conditions being met that are aimed at ensuring the safety of the PSU's data, and which are:

- the data that can be accessed through the exemption has to be limited in scope;
- the ASPSP has to apply SCA for the first access and renew it periodically, and;
- the possibility for the ASPSP to revert, at any time, to SCA if it has objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access.

For the other, separate cases where customers access the data directly, the EBA is proposing to retain the exemption in Article 10 to be voluntary as is currently the case, as no specific issues have been identified in such cases.

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

The BSG welcomes the opportunity to comment on the draft guidelines.

General Comments

The BSG considers the period for consultation too short and not sufficiently motivated when it refers to the urgency of addressing the issues at stake. The BSG recognises that EBA is trying to balance different policy objectives in its proposal. However, a mandatory exemption coupled with an extended time period could mean a reduced level of security and potentially increased risk of intentionally and/or unintentionally unauthorized access to data. Hence, a solution like this should be carefully designed and a thorough analysis is needed. We believe that if these new requirements are wrongfully calibrated, they can have a negative effect on customer trust in Open Finance, thereby delaying investments and hampering innovation and technological development.

As stated in the EBA Public Statement on Consultation Practices - EBA BS 2012 182 (II) (EBA DC 57-Annex1), the EBA will generally aim at allowing a three-month consultation period for public consultation, unless reasons exist to the contrary, for example an external timetable is imposed or the measure requires urgent action. As there are not clear reasons that motivate the urgency of this new proposed amendment, the BSG considers this consultation period too short given that from this amendment, even if motivated by the consumer interest, new risks to consumers can emerge.

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?

In principle we can see a logic to the proposal EBA has made. It is important that consumers are able to use the services provided by account information service providers without encountering an interface so unwieldy that it acts as a deterrent. We recognise that the exemption is designed to enable access only to a very limited subset of information, and not to full account functionality. As a result, security considerations should be proportionate to what could be a lower risk to consumers than relaxing SCA where their full account information is accessible. However, we suspect that in practice the extent of the risk depends on some additional assumptions that we have not been able to verify in the time available:

1. that ASPSPs' IT systems 'ringfence' the limited data from the more sensitive payment data, such that access to the limited part does not make it easier to access the other data;

2. that the more limited information is not sufficient for prevalent fraud typologies to be viable;

3. that making the exemption mandatory and extending it to 180 days would not increase the risk to consumers who are using payment initiation services from the same provider as the account information services. We are not clear how usual that is, but would see the risk to customers increasing significantly if in practice the exemption from SCA enabled any third party getting access to the account to initiate transactions too.

We therefore recommend that:

- EBA provide assurance that it has or will explicitly consider with input from NCAs, and FIUs if necessary, whether there are fraud typologies that have emerged/increased in prevalence during the pandemic that could be exacerbated by making this change in the forthcoming period;

- EBA clarify whether the exemption would apply where an AISP is 'bundling' account information with other payment services and any additional safeguards needed to ensure consumers are appropriately protected from any increased risk of unauthorized payment initiation;

- EBA consider whether further specification is needed of the definition of 'sensitive payment data' that currently only appears in Level 1 in order to appropriately delimit the scope of the exemption. [Note: the definition from Directive (EU) 2015/2366 Art 4 is as follows:

> (32) 'sensitive payment data' means data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data]

Too early to jump to conclusions

The proposed new mandatory exemption for the information accessed through an AISP and the proposed amendments to the Article 10 exemption implies that there is a need for the exemption to be made mandatory.

In our opinion however, it is too early to make this assessment as EBA has not presented concrete evidence identifying the need for such changes. This as the PSD2 RTS was applicable from the 14th of September 2019 and it took ASPSPs almost one year to initiate aggregation activity in the dedicated interface and use of 90-day exemption. Hence, a more thorough analysis is necessary to identify:

- if such a change is required by consumers,
- if the change could facilitate the failure to protect the security of the payment service user's data, increasing the privacy exposure of consumers and the ASPSP's liability resulting from unauthorised or fraudulent access, and;
- that any reduction in the security aspects of consumer protection are proportionate to the consumer benefits.

Ensuring market integrity, fair competition and customer trust

A more thorough analysis of the pros and cons of the proposal would ensure that trust for open payments – for all types of PSP is maintained. We believe that if these new requirements are wrongfully calibrated, it can have a negative effect on customer trust in the Open Payments industry, thereby delaying investments or impairing investments and hampering innovation and technological development. To strengthen competition, we see a need for measures that increase the confidence and trust in all PSPs in the value chain no matter their category to ensure that we accumulate long-term trust for all players. It cannot be ruled out that if a real and pressing need indeed could be concluded a more appropriate solution would be to let the payment service user decide about enabling an exemption or not on an individual basis.

In its current form, the suggested exemption will mainly benefit one type of PSP i.e. the AISP. This can therefore from a competition perspective be considered as distorting competition and deviating from the principle of "same activity, same risk, same rules". Further, if the exemption should be mandatory technical limitations would make it feasible only for the dedicated interface(s) and not for the customer interfaces. This is due to that it would be technically difficult, or even impossible, to implement without severely lowering the level of customer protection and ensuring that an ASPSP can fulfil its obligations to the customer as set in GDPR. However, on a positive note, if the exemption would be mandatory also for the customer interfaces this could create incentives for TPPs to fully integrate and use the provided dedicated interfaces.

If a mandatory exemption is applied when the account information is accessed through an AISP, it should be clear that the user has the possibility to revoke the access not only from the AISP but also from his/her ASPSP interface. The EBA has already mentioned before (i.e. in the Final Report on Draft RTS on SCA and CSC - EBA/RTS/2017/02 of 23 February 2017, page 85) that is of the view that *the user can always revoke the access from an AISP or ASPSP under PSD2* but if the exemption becomes mandatory this possibility should be made clear to all parties involved.

The level of risk increases in parallel with the number of days without SCA

The EBA BSG sees increased customer integrity risks coming from a mandatory exemption. If a PSU would download a token on a device, any other user using that same device will be able to access the financial data of that PSU 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.

Enhance consumer's rights to indicate no exemption

Similar to what is possible for direct debits, it would be for the benefit of consumers if they are allowed to indicate if they want SCA to be applied for a specific AISP. To that end, we would suggest the following addition (in bold and italic) to the proposed wording for Article 10a(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 ***or if the user has requested it***."

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

The EBA BSG neither supports nor dismisses the proposal to extend the deadline. The EBA has already evaluated the proposal of extending the timeline in its answer to question no 67 of the final report on

draft RTS on SCA an CSC EBA/RTS/2017/02 from 23 February 2017 stating that *"The EBA considers that 90 days is an appropriate balance between consumer-friendliness and ease of use, on the one hand, and security, on the other."*

Applying SCA two or four times a year should not make a difference. If it really does make a difference for the customer this needs to be carefully motivated to ensure long term consumer protection and trust of the Open Banking industry. However, more substantial evidence should be provided that customers indeed are requesting the proposed change and that such a change would benefit them.

One question that arises is whether there is a need to both make the use of the exemption mandatory and also extend the duration to 180 days. It may be that a mandatory 90-day exception would be sufficient. In an ideal world EBA would not be constrained by the logistics of the legislative process to have to implement both steps at the same time, but could perhaps be empowered to increase the duration of the exemption later if it proved that a mandatory exemption were not sufficient to address the problem identified.

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?

Yes: two comments.

First, we understand that EBA's intention is that ASPSPs should be required to make changes before the application date specified in Article 3(2) and should give at least a month's notices before that date of what the changes are. This intention seems appropriate but we are concerned that the current drafting of Article 2, which refers only to making the change available one month 'before implementation', with no reference to the date in Article 3(2) could give rise to a view that the implementation could take place later. We would suggest that this is clarified.

Second, we recognise that EBA does not control the precise timelines for finalising the RTS, but we would urge it to collaborate with the Commission to ensure that the application date does not require PSPs to make systems changes over the Christmas and New Year period. Many firms have IT change freezes over that time and requiring change then increases risk to all parties. Consideration should also be given to whether certain dates are easier to manage than others in relation to IT change (e.g. weekend rather than midweek).