PayBelgium

Response to the EBA consultation
(EBA/CP/2021/32)
on
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
("**RTS SCA & CSC**")

24 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?

No. PayBelgium and its members very much welcome the amendments to the RTS SCA & CSC that the EBA are suggesting in their consultation paper. We would like to thank the EBA for this important effort to improve the current situation for AISPs.

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

We very much welcome this proposal which, in combination with the mandatory application of the exemption, would already greatly improve the situation for AISPs and their customers. While we would clearly prefer an approach where there is no need for the customer to renew their consent through SCA with the ASPSP, at least in use cases where the AISP retrieves the account information without the customer being present, we understand that the EBA are of the firm view that such approach is incompatible with the PSD2 in its current form. We are therefore not requesting the EBA to reconsider this approach in the context of this consultation. Instead, we are merely sharing, in the additional statement below, why we believe it is justified for that approach to be considered in the context of the wider discussion on the review of the PSD2.

Within the context of this consultation, we understand the current view to be that the renewal of consent through SCA with the ASPSP is required to strike the balance between the objectives of the PSD2 to enhance innovation on the one hand and to protect consumers and their data on the other hand. However, the balance must be struck correctly, weighing the detrimental impact of the renewal requirement on the business of AISPs carefully against the risks their services effectively pose for consumers. We agree with the EBA that a 180-days renewal period strikes that balance more

effectively, and would still allow ASPSPs to revert to SCA at any time if they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access.

We do think however that one should distinguish between the situation where the customer is a consumer and the situation where the services are provided in a B2B context, i.e. with respect to corporate accounts or business accounts. In a B2B context the consumer protection argument plays less while the adverse impact on the AISPs' business is even greater. Indeed, the higher number of accounts that are usually involved in that context make the current consent renewal requirement even more burdensome, resulting in an even greater loss of customers.

Our members believe the EBA do not sufficiently acknowledge the distinction between those situations where they state, in paragraph 42 of their consultation paper, that "*in the EBA's view, this proposal [of a 180-days renewal period] also strikes an appropriate balance between the current timeline of 90 days which was considered as being too short, and a longer timeline of one year, or more, as suggested by some market participants, which the EBA would consider to be too long from a consumer protection perspective.*"

We therefore kindly request the EBA to reconsider the issue and to acknowledge that a consent renewal period of one year (365/366 days) would be justified in a B2B context.

Finally, if they were to prolong the 90-days renewal period, we also kindly request the EBA to consider prolonging the limitation to the 90-day transaction history in article 10.1 (b) RTS SCA &CSC accordingly.

ADDITIONAL STATEMENT: PayBelgium's view on the consent renewal requirement in an AISP context beyond the scope of this consultation, that is, for the sake of the wider discussion on the review of the PSD2

We would like to take this opportunity to single out and evaluate the two provisions of the PSD2 level 1 text that we think have led to the current interpretation that in cases where an AISP retrieves account information without the customer being present (that is, in cases where the AISP – with the consent of the customer – carries out regular background refreshes to be able to provide their services to the customer, for instance in the context of an accounting application or financial management services) the customer must also regularly renew their consent through SCA with the ASPSP:

- First, article 97.1 (a) PSD2 provides that, as a principle, SCA is required when the customer accesses their payment account online. Although technically one could argue that in an AIS context this provision only applies to situations where the customer is actively requesting the account information (Article 97.4 PSD2 provides that the principle also applies where information is requested "through an AISP", which technically is not the same as the situation where the information is requested by an AISP without the involvement of the customer), we understand that the idea of customer/data protection that underlies this principle is construed to also apply in the situation where the AISP is retrieving account information without the customer being present. Therefore, once the customer has set up the connection with the AISP, the latter can only continue to access the account information without the customer being present if the ASPSP chooses to apply the exemption of article 10 RTS SCA &

CSC and all conditions of that exemption are met, including that the access be limited to 90 days transaction history and that, for continued access, the customer renew their consent every 90 days.

- Second, article 97.5 and article 67.2 (b) PSD2 imply that, as a rule, it is the ASPSP that performs the SCA, whether it concerns the initial SCA required to connect the customer's payment account to the application of the AISP or any subsequent SCA required to renew the customer's consent.

Those provisions, and their combined application in the situation where an AISP retrieves account information without the customer being present, are truly problematic for the following reasons:

- From a business perspective, the requirements result in significant customer drop-off, with AISPs losing customers who fail to reauthenticate for a variety of mostly technical and behavioural reasons, not because of a low service value; in that sense, the provisions go against the objective of the PSD2 to enhance innovation and are having a detrimental impact on the very services the PSD2 is meant to promote;
- More importantly, we are of the view that the provisions are not justified by the other objective of the PSD2 to protect consumers and their data. We fail to see the inherent fraud risk related to the mere access to an online account and the mere viewing of transaction data, and it seems that the ECB was of the same view when they first introduced the SCA requirement in 2013 in their recommendations for the security of internet payments. Indeed, a guiding principle underlying their report is that SCA is required to protect the initiation of internet payments as well as access to sensitive payment data. For the purposes of their report, "sensitive payment data" are defined as "*data which could be used to carry out fraud. These include data enabling a payment order to be initiated, data used for authentication, data used for ordering payment instruments or authentication tools to be sent to customers, as well as data, parameters and software which, if modified, may affect the legitimate party's ability to verify payment transactions, authorise e-mandates or control the account such as "black" and "white" lists, customer-defined limits, etc.*" Moreover, in their report, the ECB explicitly stated (recommendation 4.8) that "*where a PSP offers purely consultative services, with no display of sensitive customer or payment information, such as payment card data, that could be easily misused to commit fraud, the PSP may adapt its authentication requirements on the basis of its risk assessment*."

Therefore, instead of the current approach, we would welcome an approach whereby (i) SCA with the ASPSP is required only once, that is, at the time the customer connects their account in an AISP context, and (ii) once that connection is made, the AISP either (a) periodically reminds the customer about their consent, allowing them to opt-out without SCA (option 1 (preferred))) or (b) manages the

renewal of consent itself (option 2). In any event, the ASPSP would be able revert to SCA if they have objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access.

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?

Our members would not object to reducing the standard 3-month notice on interface changes to one month or even less. However, given the importance of this issue for our members (due to the detrimental impact of the consent renewal through SCA on their client base), they suggest that the implementation timeline for ASPSPs also be reduced to a maximum of three months.

About PayBelgium

PayBelgium is the voice of the Belgian payments industry, representing the interests of payment service providers to policymakers and broader stakeholders. We are committed to uniting the industry by fostering networking and knowledge-sharing among our membership.