Single Rulebook Q&A

Question ID	2022_6526
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	72
Paragraph	-
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Not applicable
Article/Paragraph	n.a.
Date of submission	22/07/2022
Published as Final Q&A	29/09/2023
Disclose name of institution / entity	No
Type of submitter	Individual
Subject matter	Evidences / Records to be stored by account servicing payment service providers (ASPSP) for payment initiation service (PIS) and account information service (AIS) requests
Question	1. Shall ASPSP keep record of PIS requests received through a PISP and evidences on the authenticity and execution of these payment transactions when SCA is managed by ASPSP ? 2. Shall ASPSP keep record of the consent of the PSU and also of the AIS requests received through an AISP ? 3. For both evidences is there any specific retention period ?
Background on the question	Article 72 specifies that when a payment is initiated through a PISP then it burdens to PISP to provide evidences on the authenticity and execution of a payment transaction. However in case an SCA exemption is not applicable and SCA is managed by ASPSP, the PISP cannot provide all evidences without relying on the ASPSP. After an authentication of a PSU, an AISP can request account informations for a period of 90 days before the renewal of the authentication. The consent of the PSU is recorded but the regulation does not contain any requirement regarding the records to keep in relation with AIS requests performed by the AISP during the consent period of 90

	days.
Final answer	In accordance with Article 64(2) of Directive 2015/2366/EU (PSD2), “Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider. Consent to execute a payment transaction may also be given via the payee or the payment initiation service provider. In the absence of consent, a payment transaction shall be considered to be unauthorised”. Furthermore, Article 64(4) of PSD2 provides that “The procedure for giving consent shall be agreed between the payer and the relevant payment service provider(s).” In accordance with Article 72 of PSD2, “where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider'. Moreover, Article 29(1) of the Commission Delegated Regulation (EU) 2018/389 (the ‘RTS on SCA&CSC') requires payment service providers (PSPs) to “have processes in place which ensure that all payment transactions and other interactions with the payment services user, with other payment service providers and with other entities, including merchants, in the context of the provision of the payment service are traceable, ensuring knowledge ex post of all events relevant to the electronic transaction in all the various stages. Article 29(2) provides that, for the purpose of Article 29(1), PSPs “shall ensure that any communication session established with the payment services user, other payment service providers and other entities, including merchants, relies among others, on “security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data”. It follows from the above that account servicing payment service providers (ASPSPs) should keep records of the authorisation of a payment transaction executed by the ASPSP, including, in the case of a transaction initiated through a payment initiation service provider (PISP), evidence regarding the request received from the PISP, as well as evidence that the ASPSP has complied with the requirements in Article 97 of PSD2 and the RTS on SCA&CSC regarding the application of strong customer authentication. ASPSPs should also keep records regarding any access requests to the payment service user (PSU)’ s payment accounts received from account information service providers (AISPs), and evidence that the ASPSP has complied with the requirements in Article 97 of PSD2 and the RTS on SCA&CSC regarding the application of strong customer authentication.

	The relevant retention periods set out in relevant Union law, and where applicable, national law, shall apply. This being said, the EBA recalls that, as clarified in paragraph 13 of the EBA Opinion on the implementation of the RTS on SCA&CSC (EBA-Op-2018-04), and paragraph 43 of the EBA Opinion on obstacles under Article 32(3) of the RTS on SCA and CSC, ASPSPs should not check the consent granted by the PSU to TPPs, and that it is the obligation of the PISP/AISP to ensure that it has obtained the PSU's explicit consent in accordance with Article 66(2) of PSD2 and, respectively, Article 67(2)(a) of PSD2.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2022_6526

European Banking Authority, 03/10/2023
www.eba.europa.eu