Single Rulebook Q&A

Question ID	2018_4440
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	74
Paragraph	-
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	Article 4 - Authentication Code
Date of submission	28/12/2018
Published as Final Q&A	17/12/2021
Disclose name of institution / entity	Yes
Name of institution / submitter	Quali-Sign Ltd
Country of incorporation / residence	UK
Type of submitter	Other
Subject matter	Revocation / Invalidation of SCA proof before execution date
Question	In order for a payment instruction to be regarded as 'authorised', is the Account Servicing Payment Service Provider (ASPSP) obliged to verify the strong customer authentication (SCA) proof immediately prior to the execution of each future dated payment instruction? If the ASPSP fails to re-verify the SCA proof, can the ASPSP hold the payer liable in the event of fraud?
Background on the question	An ASPSP establishes an SCA procedure for their corporate customers that adopts best practice techniques laid out by the EU's eIDAS regulation. . Business Payment Service User (PSU)'s that prepare files of payments within their enterprise resource planning (ERP) package are recommended to apply a company seal (electronic signature) with a commitment type of #proofOfCreation, before combining the payment order data and signature

	into an 'Associated Signature Container' (ASiC) for transmission to the ASPSP. On receipt, the ASPSP routes the payment order into its 'decoupled SCA procedure', whereby one or more personal authorisation PSU's are requested to approve the payment order on behalf of the business PSU. As there can be many payment instructions within a file, the approver must rely on the #proofOfCreation as evidence that the instructions have not been maliciously modified, since creation. Personal approval is captured via the creation of electronic signatures with a commitment type of #proofOfApproval. These additional signatures are added to the ASiC. The ASiC represents unambiguous and demonstrable evidence of explicit consent to execute the related payment instructions.With respect to IT Security threats, the business PSU's must work on the assumption that their systems have already been breached. They must plan for the possibility that the integrity of the systems that create the payments are compromised. This would undermine the integrity of the #proofOfCreation. It is essential that the business PSU's understand how to quickly invalidate/revoke the SCA proof for any future dated payment instructions that have already been transmitted to the ASPSP, but have not yet been booked. It is also essential that the business PSU understands their (payer) liability and right of recourse, in the event of fraud.
Final answer	Article 64(1) of Directive 2015/2366/EU (PSD2) provides that “Member States shall ensure that a payment transaction is considered to be authorised only if the payer has given consent to execute the payment transaction” and that “a payment transaction may be authorised by the payer prior to or, if agreed between the payer and the payment service provider, after the execution of the payment transaction”. Article 64(2) and (4) of PSD2 further specifies that “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” and that “the procedure for giving consent shall be agreed between the payer and the relevant payment service provider(s)”. Therefore, the procedure for giving consent, including the steps that the payment service provider (PSP) should take to check whether the transaction has been authorised, depends on what has been agreed between the payment service user (PSU) and that PSP. With regard to the execution of future dated transactions, Q&A 4795 clarified that strong customer authentication (SCA) may be applied in advance of a future-dated payment transaction and that the PSD2 and the Commission Delegated Regulation (EU) 2018/389 do not specify a timeframe for the validity of an SCA applied at the time when a payer initiates an electronic payment transaction.

	Relatedly, where SCA is applied in advance of a future-dated payment transaction, PSD2 and the Delegated Regulation do not require SCA to be re-applied (or verified) before the future-dated payment transaction is executed. Therefore, in the case described by the submitter, the need to verify the SCA proof immediately prior to the execution of each future dated payment instruction will depend on the agreement between the PSU and the PSP.
Link	https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4440

European Banking Authority, 20/05/2022
www.eba.europa.eu