Single Rulebook Q&A

Question ID	2020_5215
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	4
Paragraph	30
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	6
Date of submission	21/04/2020
Published as Final Q&A	05/11/2021
Disclose name of institution / entity	No
Type of submitter	Credit institution
Subject matter	Elements of possession (SIM card) and knowledge (knowledge-based responses to challenges or questions)
Question	1. Can evidence of possession (SIM card) can also be verified by reading and identifying the phone number used for the phone call? 2. Can a knowledge element be based on a) transaction history of the customer; b) contact information of the customer?
Background on the question	Customers use telephone bank (by calling to customer service unit) to initiate payment transactions and/or perform other actions which imply risk of payment fraud or other abuses. It is our understanding that PSD2 Art.97 (1) (b) and (c) therefore requires to apply Strong customer authentication (SCA). During a phone call, the operator receiving the call sees the phone number used for the call and therefore can identify and verify that the same phone number is registered in the system of the bank, which evidences the possession element. To evidence the knowledge element, the customer may be asked a set of questions which are based on a) customer's transaction history (e.g. amount of last transaction; place of last transaction at ATM; number of opened accounts; date of establishing business relationships; last internetbank login date etc.) and b) customer's contact information

	registered with the institution (e.g. mailing address; e-mail address; workplace; internetbank login etc.). Point 25 and item 1 of the Table 2 of the EBA Opinion on the elements of strong customer authentication under PSD2, EBA-Op-2019-06, refers to "Possession of a device evidenced by an One Time Password (OTP) generated by, or received on, a device (hardware or software token generator, SMS OTP)" Point 32 and item 3 of the Table 3 of EBA-Op-2019-06 refers to "Knowledge-based responses to challenges or questions" as an element constituting the element of knowledge under PSD2 Art.4 (30).
EBA answer	Article 97(1)(b) of Directive 2015/2366/EU (PSD2) prescribes that payment service providers (PSPs) shall apply strong customer authentication (SCA) where the payer initiates an electronic payment transaction. Recital 95 of PSD2 clarifies that 'all payment services offered electronically should be carried out in a secure manner, adopting technologies able to guarantee the safe authentication of the user and to reduce, to the maximum extent possible, the risk of fraud. There does not seem to be a need to guarantee the same level of protection to payment transactions initiated and executed with modalities other than the use of electronic platforms or devices, such as paper-based payment transactions, mail orders or telephone orders.' Q&A 2019_4788 further clarified that 'remote non-electronic payment transactions that are initiated and executed via a mail order or telephone order can be considered out of scope of the SCA requirement. Therefore, as card-based payment transactions qualify as electronic payment transactions, card-based transactions initiated by the payer through the payee cannot be considered out of scope of the SCA requirement'. Accordingly, the payment transaction described by the submitter may fall outside the scope of the SCA requirements only if it is a non-electronic payment transaction initiated and executed with the PSP only via a telephone order. Otherwise the application of SCA will be required. With regard to the specific case described by the submitter where staff of the PSP verifies the identity of the payment service user (PSU) over a telephone call by (i) reading the telephone number used for the call and (ii) asking for information on transaction history or contact information, the SCA requirements under PSD2 and the Commission Delegated Regulation (EU) 2018/389 will not be met. While verifying the telephone number used for the call may evidence possession (of the SIM-card associated with the respective telephone number) if the requirements of Article 7 of the Delegated Regulation are met, the transaction history and/or the contact details information of the PSU cannot constitute a knowledge element since this information will be available to members of staff of the PSP and potentially to other parties, and

	so does not meet the requirements of Article 6 of the Delegated Regulation and Article 4(30) of PSD2, which prescribes that knowledge is ‘something only the user knows’. Accordingly, authentication based on the combination of reading the telephone number used for the call and asking for information on transaction history or contact information will not be a valid two-factor SCA under PSD2 and the Delegated Regulation.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5215

European Banking Authority, 21/01/2022
www.eba.europa.eu