Single Rulebook Q&A

Question ID	2019_4937
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	97
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	1-4
Date of submission	07/10/2019
Published as Final Q&A	25/09/2020
Disclose name of institution / entity	No
Type of submitter	Individual
Subject matter	SCA for contactless payments at a POS executed via a mobile device
Question	1) Can we consider the strong customer authentication (SCA) outsourced from the issuer of cards to the payer? 2) Is it necessary for the issuer of the cards to perform SCA based on the elements of identification that are beyond its control?
Background on the question	Whereas the following transactions having the cumulative characteristics: - In case of contactless payment (irrespective of the value) executed at a POS (point of sale); - Payments executed through a mobile device (phone, watch etc.) - The mobile device is owned by the payer; - The payer enrolls its cards in an electronic wallet downloaded on the device (e.g. an application) which is provided by a supplier of such software; - After the enrolment of cards within the wallet performed by the payer, the issuer of cards will verify the identity of the cardholder and the link between the cardholder and the enrolled cards and furthermore authorizes the enrolment of cards chosen by the payer; - The payer shall establish at the enrolment moment the security elements needed for the payments (e.g. device lock screens, fingerprint, face ID, passcode of the

	phone/application etc.), hereinafter referred as ”elements of identifications”; - The payer is the only one able to set up its own method of identification and verification for authorization of payments with one of the elements of identifications mentioned above; - The payer is the only one able to change the settings of the above mentioned elements of identifications due to the fact that has the control of his own device; - The elements of identifications are hosted in the mobile device’ memory and are beyond the control of the issuer of cards.
EBA answer	Article 97(1) of Directive 2015/2366/EU (PSD2) requires payment service providers (PSPs) to ‘apply strong customer authentication where the payer: (a) accesses its payment account online; (b) initiates an electronic payment transaction; (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.’ Article 4(29) of PSD2 defines authentication as ‘a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user’s personalised security credentials’. The Commission Delegated Regulation (EU) 2018/389 introduces several exemptions from the application of strong customer authentication (SCA) under Articles 11 – 18 of the Delegated Regulation, such as Article 11 exemption on the contactless payments at point of sale. In relation to the above, unless the exemption under Article 11 of the Delegated Regulation or another exemption from the application of SCA applies, payment service providers (PSPs) should apply SCA to contactless payments at a point of sale terminal executed via a mobile device. Q&A 2018_4047 clarified that issuing PSPs may (i) use third party technology, such as a smartphone fingerprint reader, to support SCA and to ensure they fulfill all the security measures established in the Delegated Regulation (EU) 2018/389 or (ii) outsource the execution of SCA to a third party in compliance with the general requirements on outsourcing, including the requirements in the EBA Guidelines on Outsourcing arrangements (EBA/GL/2019/02). This Q&A further clarified ‘the responsibility for compliance with SCA cannot be outsourced from PSPs to third parties and that PSPs remain fully responsible for the compliance with the requirements in the Delegated Regulation.’ With regard to the above, while the PSP may outsource the execution of SCA to a third party, this does not include the payer of the payment

	transaction, since, in accordance with Article 4(29) of PSD2, authentication is a procedure verifying the identity of the payment service user and consequently cannot be managed by the payment service users themselves, including because this would give rise to security risks, such as identity theft and fraud. Q&A 2018_4047, Q&A 2019_4560 and Q&A 2019_4651 provide further details on the use of SCA elements stored on authentication devices.
Link	https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4937

European Banking Authority, 07/11/2020
www.eba.europa.eu