Single Rulebook Q&A

Question ID	2019_4651
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	98
Paragraph	1
Subparagraph	d
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	8/1
Date of submission	01/04/2019
Published as Final Q&A	25/09/2020
Disclose name of institution / entity	No
Type of submitter	Law firm
Subject matter	Relying on vendor mechanisms processing the biometric data for strong customer authentication; Multiple fingerprint samples stored on a mobile device and used for purpose of user authentication.
Question	Are the obligations of a payment service provider (PSP) laid down in the Article 8 of RTS on strong customer authentication and secure communication fulfilled in case the biometric credentials of customer are stored at the device level and the strong customer authentication itself is processed by the mobile device? In this context, are the obligations of the PSP laid down in Article 8 and 24 of RTS on Strong Customer Authentication fulfilled in case the mobile device stores multiple fingerprint samples for user authentication?
Background on the question	Article 8 paragraph 1 of the EU Commission Delegated Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication provides that the PSP shall adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a minimum, the PSP shall ensure that those

	access devices and software have a very low probability of an unauthorised party being authenticated as the payer. In case customers intend to use fingerprint or facial recognition as inherence element to access their payment account online through mobile banking application on a mobile device which runs on iOS or Android operating system, the mobile banking application uses the fingerprint or facial recognition system implemented on the Android or iOS operating system. In such case, the biometric data of the respective customer are stored on the secure enclave of a mobile device and the biometric authentication itself is processed by the operating system of the respective mobile device. PSP itself does not have access to biometric data of the customer, but only obtains positive or negative result of the user verification (i.e. whether the verification was successful or not). No application has access to the secure enclave where the biometric data are stored. As a result, the PSP has to rely on the vendor mechanisms (e.g. in case of iOS Apple touch ID) for customer identity verification including the implemented security measures. Pursuant to Article 24 of RTS on Strong Customer Authentication, the PSP should ensure that only the payment service user is associated, in a secure manner, with the personalized security credentials, the authentication devices and the software. However, some fingerprint recognition software implemented on a mobile device demand multiple fingerprint samples for user verification and therefore, there is a risk that fingerprint samples of multiple persons could be stored on the mobile device even before installation and registration of a mobile banking application. Under such conditions, the PSP cannot ensure with certainty that another person will register and use the mobile banking application on behalf of the actual payment services user.
EBA answer	Q&A 2018_4047 clarified that issuing payment service providers (PSPs) may (i) use third party technology, such as a smartphone fingerprint reader, to support strong customer authentication (SCA) and to ensure they fulfill all the security measures established in the Commission 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 that PSPs remain fully responsible for the compliance with the requirements in the Delegated Regulation and that PSPs should make sure that the technical service provider has a satisfactory level of security and that it applies the mitigating measures in accordance with Article 9 of the Delegated Regulation. The security measures referred to in the answer to Q&A 2018_4047 include the requirements of Article 8 of the Delegated Regulation. This means that PSPs may, in line with the requirements of Article 8 of the Delegated Regulation, use biometric credentials that are stored at the

	device level for the application of the strong customer authentication, provided that the PSPs has ensured that technology used has a satisfactory level of security. Q&A 2019_4560 provides further clarity on the use of an authentication device by multiple users, including on the association of the personalised security credentials, such as a fingerprint. In line with Article 24 of the Delegated Regulation and the answer to Q&A 2019_4560, in case the authentication device can store multiple fingerprint samples that are used as personalised security credentials, the PSP should ensure that only a single payment service user (and their SCA profile) is associated with their respective fingerprint samples.
Link	https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4651

European Banking Authority, 14/10/2020
www.eba.europa.eu