Single Rulebook Q&A

Question ID	2019_4875
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	1
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 Paragraph 3(a)
Date of submission	16/08/2019
Published as Final Q&A	25/09/2020
Disclose name of institution / entity	No
Type of submitter	Consultancy firm
Subject matter	Failed Authentication Code
Question	Please clarify under what circumstances Article 4 Paragraph 3(a) of the Regulation (EU) 2018/389 – RTS on SCA and SC might it be impossible to apply in remote authentication where SMS based One time passwords (OTPs) are used as the authentication method.
Background on the question	I wish to clarify my interpretation of Article 4 Paragraph 3(a) of the Regulation (EU) 2018/389 – RTS on SCA and SC. This is because the failure to generate an authentication code will always show that the knowledge element of the authentication (the customer's ID and Password combination) will be exposed to an attacker The common interpretation of Article 4 Paragraph 3(a) is that it is referring to what is often called in the information security community as preventing "verbose reporting". In other words preventing extraneous detail being presented on a failed log-on that might impart information to an attacker to refine his attack. As I stated this is a sound control to have in most computer systems during a log-on process. The reason that implementing SMS based OTP may find it impossible to meet this article is that it must be a two step process. One can never make SMS OTP a single authentication step where both

	knowledge and Authentication Code are presented at the same time. In the first step there is some form of authentication based on an ID and password before the SMS OTP is sent to the customer. This is necessary because the entity authenticating the customer first needs to conduct an internal look-up to recover the user’s mobile telephone number that has been registered for that account in order to send the SMS OTP authentication code to that user. Therefore the entire authentication exchange taking place fails to meet the intent of this article because the attacker will gather information during his attack; namely that the ID and password combination are in sufficient for him to be sent an authentication code. However it is true to say that an SMS OTP authentication solution can met the intent of this article for the initial ID and password check to request an SMS OTP authentication code.
EBA answer	In accordance with Article 4(a) of the Commission Delegated Regulation (EU) 2018/389, “where payment service providers apply strong customer authentication [SCA] in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code”. Article 4(3)(a) of the Delegated Regulation further provides that payment service providers shall ensure that “where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, it shall not be possible to identify which of the elements referred to in that paragraph was incorrect.” Q&A 2018_4041 clarified the application of Article 4(3)(a) of the Delegated Regulation, in particular that payment service providers should not provide any indication on which element was incorrect. This also applies to the case described by the submitter with a two-step authentication process based on a password, as a knowledge element, and an SMS OTP evidencing the possession element.
Link	https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4875

European Banking Authority, 03/11/2020
www.eba.europa.eu