Single Rulebook Q&A

Question ID	2019_4662
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	-
Subparagraph	-
COM Delegated or Implementing Acts/RTS/ITS/GLs/Recommendations	Regulation (EU) 2018/389 - RTS on strong customer authentication and secure communication
Article/Paragraph	4.3 (b)
Date of submission	09/04/2019
Published as Final Q&A	19/06/2020
Disclose name of institution / entity	Yes
Name of institution / submitter	Fido alliance
Country of incorporation / residence	France
Type of submitter	Industry association
Subject matter	Define what is “given period of time”
Question	What constitutes a “given period of time” as expressed in Article 4.3 (b) of the RTS on strong customer authentication and secure communication?
Background on the question	RTS Article 4.3 (b) states “the number of failed authentication attempts that can take place consecutively, after which the actions referred to in Article 97(1) of Directive (EU) 2015/2366 shall be temporarily or permanently blocked, shall not exceed five within a given period of time;”.It is assumed that the goal of the requirement is to rate-limit, for example, of the brute force attacks to an acceptable level of security.
EBA answer	In accordance with Article 4(3)(b) of the Delegated Regulation (EU) 2018/389, payment service providers (PSPs) shall ensure that the actions referred to in Article 97(1) of Directive 2015/2366/EU (PSD2) are temporarily or permanently blocked after a number of failed

	authentication attempts that does not exceed five within a given period of time. The Delegated Regulation does not specify the time period during which the failed authentication attempts referred to in Article 4(3)(b) shall take place. Therefore, it is for each PSP to decide, based on their risk assessment, the duration of this time period. The same principle applies also to determine the duration of the temporary block of the actions, referred to in Article 97(1) of PSD2, by the PSP after the maximum number of failed authentication attempts has been exceeded, or when the PSP should block these actions permanently.
Link	https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4662

European Banking Authority, 11/08/2020
www.eba.europa.eu