Single Rulebook Q&A

Question ID	2020_5621
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	6, 7, 8, 9
Date of submission	16/11/2020
Published as Final Q&A	23/04/2021
Disclose name of institution / entity	No
Type of submitter	Other
Subject matter	Use of new technology for SCA
Question	Is a Payment Services Provider (PSP) allowed to adopt innovative technologies for verifying Payment Services Users (PSUs) where the PSP maintains fraud levels below a certain threshold?
Background on the question	The rules for applying Strong customer authentication (SCA) are technology and business model neutral and have been designed to reduce fraud associated with electronic transactions. However, to ensure compliance,

	some PSPs have started adopting SCA solutions that fulfil the technical requirements for SCA but do not necessarily reduce fraud or increase the security of payments. Some of these solutions are susceptible to fraud, and while they offer a means of verifying a PSU, they do not provide increased security or fraud prevention to the PSU. There are innovative solutions that offer a different way of verifying instructions from PSUs while enhancing the security of electronic transactions. These solutions rely on innovative technologies (such as machine learning) to reduce fraudulent transactions. For instance, they can be used to identify fraudulent devices, IP addresses and locations, as well as fraudulent security credentials resulting in a robust way of mitigating and preventing potential fraud. Some of these solutions do not necessarily fit into the strict categories of possession, knowledge or inherence, because they rely on advanced machine learning and data analytics, to identify and prevent fraudulent instructions or transactions from suspicious sources. Since the rules of SCA are technology and business model neutral, new and innovative approaches (such as advanced machine learning and data analytics) which reduce fraud, should be allowed as an option for PSPs to verify instructions from PSUs.
EBA answer	In accordance with Article 97(1) Directive 2015/2366/EU (PSD2), payment service providers (PSPs) shall apply strong customer authentication (SCA) when the payer (a) accesses its payment account online, (b) initiates an electronic payment transaction, or (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. Article 4(30) of PSD2 defines strong customer authentication as 'an authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data'. The Commission Delegated Regulation (EU) 2018/389 provides further details on the requirements for SCA. PSD2 and the Delegated Regulation do not restrict PSPs from using additional security measures to the application of SCA, which would not constitute a valid element of SCA by themselves, such as those referred to by the submitter, namely solutions relying on innovative technologies (such as machine learning) to identify fraudulent devices, IP addresses and locations, as well as fraudulent security credentials. Article 2 of the Delegated Regulation, in particular, requires PSPs to adopt transaction monitoring mechanisms 'that enable them to detect unauthorised or fraudulent payment transactions for the purpose of the implementation of the security measures'.

Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5621

European Banking Authority, 03/05/2021
www.eba.europa.eu