Single Rulebook Q&A

Question ID	2020_5325
Status	Final Q&A
Legal act	Directive 2015/2366/EU (PSD2)
Topic	Strong customer authentication and common and secure communication (incl. access)
Article	97 & 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	all
Date of submission	21/06/2020
Published as Final Q&A	17/12/2021
Disclose name of institution / entity	Yes
Name of institution / submitter	Any
Country of incorporation / residence	Spain
Type of submitter	Individual
Subject matter	Alternative strong customer authentication for citizens without mobile
Question	Why does the PSD2 allow banks to deny the access to the electronic financial services to customers without a mobile but with a PC?
Background on the question	In Member State A, bank customers only can log in their accounts with username or ID number + pin code or password + SMS one time password.I do not have a mobile. However, I do have, a PC, which I have been using for electronic bank transactions for 20 years with a bank pin card. I cannot buy anything through the internet with my credit/debit cards since 2016. I cannot make any electronic bank transaction since September 2019. I cannot even log in my bank account since January 2020.I am not against the Strong customer authentication (SCA) methods and I know EBA developed those SCA methods under the principle of “technological neutrality”.However, since PSD2 does not force banks to apply a particular SCA method, should

	not the PSD2 make banks implement a range of SCA methods to ensure that all bank consumers have access to digital financial services regardless of the kind of electronic devices they own or not?I believe that I have the right to use electronic financial services and in spite of having a PC I do not have access to such services because I do not have a mobile, so all banks in Member State A are discriminating against their customers based on owning or not a mobile.The RTS does not specifically mention anything about banks and Payment Service Providers (PSPs) guarantee that users are able to access and perform electronic transaction independently of kind of electronic device they have. This is something that it is not covered in the regulations and thus, in Member State A, the Banks and PSPs have limited such transactions only to user with a mobile, since having a mobile is compulsory.Point (4) of the first page of Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication states “To remain technologically neutral a specific technology for the implementation of authentication codes should not be required”.If a specific technology is not required to implement the authentication codes, why do all the Member State A’s banks require customers to have a mobile?I believe any kind of discrimination (in this case versus people not having a mobile) should be avoided, and it seems that the only way to get it is through being included in the regulations.Maybe the regulation should specify that banks and PSPs should implement different SCAs for customers with a mobile and without a mobile but with a different electronic device in order to avoid this situation.The RTS is mainly focused in customer protection but not in assuring that all customer owning an electronic device different from mobile get access to the electronic payments.That, at least in Member State A, has resulted in excluding users with only a PC or a tablet access to electronic transactions. In my case, I have been using only a PC for my electronic financial transactions during 20 years with two different authentication methods (one I know and one I possess).Since January 2020, I do not have access and I do not understand why because I was already using two authentication methods.
Final answer	ArticleA 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(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’. PSD2 and the Commission Delegated Regulation (EU) 2018/389 do not prescribe a specific authentication approach that should be used for applying strong customer authentication. It is left for payment service providers to choose how to authenticate their customers. Finally, he EBA has provided in its Opinion on the elements of strong customer authentication (EBA-Op-2019-06) non-exhaustive lists of possible elements of strong customer authentication (knowledge, possession and inherence) that comply or may comply with the legal requirements. These lists include authentication elements that are not based on mobile phones and mobile applications.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5325

European Banking Authority, 20/05/2022
www.eba.europa.eu