Single Rulebook Q&A

Question ID	2018_4135
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
Date of submission	18/07/2018
Published as Final Q&A	15/01/2021
Disclose name of institution / entity	Yes
Name of institution / submitter	Banque de France
Country of incorporation / residence	France
Type of submitter	Competent authority
Subject matter	SMS OTP and credit card as a two authentication factor
Question	Can we consider Credit card and One Time Password (OTP) SMS as a two authentication factor ?
Background on the question	The main authentication solution for online card payments deployed in France is based on sending a single-use confidential code by SMS to the bearer of the card, in addition to the payment card data entry (number, expiry date, cryptogram,even name and surname of the bearer). (Known as 3d-secure) for electronic payment.EBA Opinion on the implementation of the RTS on SCA and CSC (Op-2018-04)- Article 36 : Given that knowledge is defined as 'something only the user knows', the card number with CVV and expiry date printed on the card cannot be considered a knowledge element.Regulation (EU) 2018/389 – RTS on strong customer authentication and secure communication, Article 6 (Requirements of the elements categorised as knowledge) :1.Payment service providers shall adopt measures to mitigate the risk that the elements of strong customer

	authentication categorised as knowledge are uncovered by, or disclosed to, unauthorised parties.2.The use by the payer of those elements shall be subject to mitigation measures in order to prevent their disclosure to unauthorised parties.
EBA answer	Paragraph 35 of the EBA Opinion on the Implementation of the RTS on SCA and CSC (EBA-Op-2018-04), stated that the card details and security code printed on the card would not constitute a knowledge element. In addition, while a card with a dynamic card security code may constitute a possession element, it would not constitute a knowledge element. Table 2 of the EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06), notes that a Card with possession evidenced by either card details (printed on the card) or by a printed element (such as an OTP list) is not a compliant 'possession' element, for approaches currently observed. In relation to the above, card details cannot be used as a valid factor in a two-factor Strong Customer Authentication (SCA) under Directive 2015/2366/EU (PSD2) and the Commission Delegated Regulation (EU) 2018/389. With regard to the SMS OTP, as clarified in Q&A 2018_4039 a one-time password sent via SMS would constitute a possession element and should therefore comply with the requirements under Article 7 of the Delegated Regulation. This was also reflected in Table 2 of the EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06).
Link	https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4135