Single Rulebook Q&A

Question ID	2020_5620
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	8
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 behavioural data for SCA
Question	Can a Payment Service Provider (PSP) use behavioural data and auditable scores to apply Strong customer authentication (SCA) in a way that protects consumer privacy?
Background on the question	The EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06), June 2019, clarified that inherence may include behavioural biometrics identifying the specific authorised user and that

	inherence relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. The EBA gave examples of factors which constitute inherence, including fingerprint and face scanning, keystroke dynamics and the angle at which a user holds the device, adding that these could be used to authenticate PSUs provided the implemented approaches have a 'very low probability of an unauthorised party being authenticated as the payer'. In order to meet the criteria of behavioural biometrics under the EBA Opinion of June 2019, PSPs may have to obtain sensitive data about a Payment Service User (PSU) to create a behavioural biometric that can be used to identify the PSU. This may include information such as how a consumer navigates on a computer or webpage, capturing keystrokes, typing style and speed and how the consumer interacts with their device. This would allow a PSP (or its provider) to create a fingerprint of an online session and compare with a historical baseline to verify a consumer. Such solutions could require PSPs and third parties to obtain information from a user's personal device (such as a computer or mobile phone) by scraping the information or installing technologies that monitor a consumer's use of a personal device. There are additional concerns over the scope and definition of behavioural biometrics in the EBA Opinion of June 2019 in that: 1) some devices used for payments have been designed to protect consumer privacy by preventing third parties from capturing or accessing sensitive information such as keystroke dynamics or fingerprints; 2) some of the browser based solutions are not compatible with purchases within apps; and 3) allowing or encouraging third parties to capture information relating to "physical properties of body parts, physiological characteristics and behavioural processes" as contemplated in the Opinion could lead to solutions that profile individuals using sensitive information in conflict with the General Data Protection Regulation (GDPR), lending this to abuse or risk of compromise by malicious actors. It is possible for PSPs to obtain behavioural data and auditable behavioural scores about a PSU's device, mobile number and account activity in a way that protects consumers' privacy while preventing / reducing fraud. This can be done without accessing or capturing sensitive information relating to an individual's physical or body parts. We welcome clarification that PSPs can use behavioural data and auditable behavioural scores about a PSUs' device, mobile number and account activity to verify a user and meet SCA requirements.
EBA answer	Article 8(1) of the Commission Delegated Regulation (EU) 2018/389 specifies that payment service providers (PSPs) 'shall adopt measures to mitigate the risk that the authentication elements categorised as inherence and read by access devices and software provided to the payer are uncovered by unauthorised parties. At a minimum, the payment service providers shall ensure that those access devices and software have a very low probability of an unauthorised party being authenticated as the payer.' Paragraph 34 of the EBA Opinion on the implementation of the RTS on SCA

	and CSC (EBA-Op-2018-04) clarified that an authentication based on inherence 'is typically based on biometrics (including behavioural biometrics), provided they comply with the requirements under Article 8 of the RTS'. Paragraph 18 of the EBA Opinion on the elements of strong customer authentication under PSD2 (EBA-Op-2019-06) further clarified that 'inherence, which includes biological and behavioural biometrics, relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body, and any combination of these. In addition, it is (the quality of) the implementation of any inherence-based approach that will determine whether or not it constitutes a compliant inherence element'. Paragraph 19 and Table 1 of the 'EBA Opinion on the elements of strong customer authentication under PSD2' provide a non-exhaustive list of possible inherence elements, which include keystroke dynamics and body movement patterns. In relation to the above, behavioural data related to the physiological characteristics and behavioural processes created by the body and auditable scores based on them, may be used as an inherence element in a strong customer authentication, provided that their implementation meets the requirements of Article 8 of the Delegated Regulation. This is without prejudice to the requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR). The examples of behavioural biometrics provided in the 'EBA Opinion on the elements of strong customer authentication under PSD2' may not be compatible with some devices and browser-based solutions. However, it is for the payment service provider to choose the authentication approaches they would apply for carrying out strong customer authentication.
Link	https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5620