# Strong Customer Authentication: Considerations for what can be used as a second factor alongside One Time Passcode (OTP)

**Date:** July 2020

This document is being issued to help card issuers (e.g. banks), technology providers and others with understanding what can be considered as a valid second factor for one-time passcode (OTP) within the construct of Strong Customer Authentication (SCA), since the European Banking Authority (EBA's) Opinion in June 2019 clarified that card details could not be considered a valid factor. In practice, this means that many card issuers will be using an OTP solution, such as a one-time passcode sent by text or via landline to comply with SCA requirements. Many will be aware this will require a second factor (either inherence or knowledge) over and above the OTP solution (possession) in order to comply with SCA.

Card issuers are advised to define their solution for their second factor as a matter of urgency (if plans are not already well progressed) and to speak with their ACS provider (if applicable). Issuers using OTP are required to ensure a two-factor compliant solution is in place by 14 September 2021.

Merchants are asked to take note of the section below addressed to them in order to facilitate the best possible user experience for their customers.

## What is Strong Customer Authentication (SCA)?

Strong Customer Authentication (SCA) is a new set of rules that will change how customers confirm their identity when making purchases online to help further protect them from fraud. Following its implementation, customers shopping, or banking online will often need to undertake an extra step to confirm their identity. For example, the card issuer or provider (like a bank) may use one of a number of ways to verify a purchase or login, such as a passcode via text message, a phone call to the consumer's landline, the use of a card reader or the use of a smartphone app. Under the new rules all parties are required to make the necessary changes to enable customers to authenticate their actions in a manner compliant with the SCA requirements.

As per the SCA rules, customers will need to be authenticated using a two-factor authentication (2FA). This means issuers will need to choose an authentication[1] method that comprises two elements out of the three SCA categories:

[1] Please refer to the Regulatory Technical Standards on strong customer authentication and common and secure open standards of communication or UK Finance's upcoming guidance for more information about the specific requirements of the strong customer authentication that should be applied each time a payer accesses its payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of payment fraud or other abuse,

- Knowledge: something only the user knows
- Possession: something only the user possesses
- Inherence: something the user is

Many issuers will be offering an authentication solution via their mobile banking app to customers that have mobile banking and are active digital users. However, to support those customers that either do not have mobile banking, or do not have access to the relevant technology, most of the UK card issuers will be also deploying an OTP.

The European Banking Authority (EBA's) Opinion in June 2019 clarified that card details could not be considered a valid factor. In practice, this position has an impact on many card issuers using an OTP solution, sent by text or via landline, to comply with SCA requirements. As this solution relies upon possession as one factor (the OTP sent to the customer's pre-registered mobile device or landline proves that the customer is in possession of the mobile device or landline). Card issuers will be aware this solution requires a second factor (either inherence or knowledge) over and above the OTP solution in order to comply with SCA.

## What options are available as a second factor?

Broadly, there are two potential solutions that have been considered by the industry, these include a behavioural biometric (inherence) solution and a knowledge-based solution which complements the existing one-time passcode (possession) factor. Please see below for more detail on these. The industry generally views behavioural biometrics as a better solution as it provides multiple benefits, including less need for action from the customer.

**The recommended industry position is the use of behavioural biometrics as the second factor in authentication, with no fall back (for scenarios where the use of behavioural biometrics is not feasible).** The Financial Conduct Authority supports the development of strategic solutions that are good for customers and businesses and has welcomed the industry's suggestion to focus on behavioural biometrics as second factor to an OTP solution.

**1. Behavioural Biometrics – Inherence (industry recommended approach)**

The usage of behavioural biometrics alongside OTP provides a compliant SCA authentication solution whilst minimising the impact to customers and merchants when shopping online. Behavioural biometrics does not require customers to use and manage a knowledge factor (like a password or a PIN) which has the potential to increase friction during checkout as well as fraud risk. Both the FCA SCA Forum and the SCA Programme Steering have acknowledged that the usage of behavioural biometrics might not be feasible in a limited number of cases. Therefore, the reduced number of transactions in this category could be authenticated using OTP plus other controls such as 3DS data profiling, which is a proven and effective method for preventing fraud.

The potential scenarios where the usage of behavioural biometrics **could represent a challenge** are:

a. Merchants apps (mobile or consumer device)
b. Journeys with embedded 3DS SDK i.e. smart TV, game console

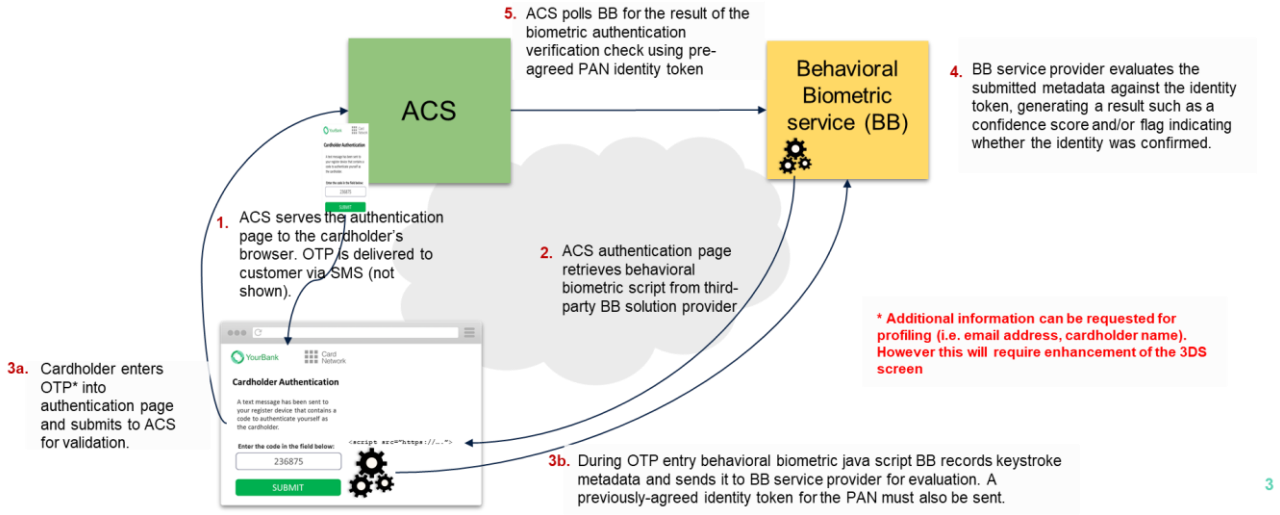
Issuers and merchants are encouraged to promote authentication via the issuer's app to ensure transactions in these categories can be authenticated in a compliant manner.

The solutions for the use of behavioural biometrics as a second factor are based on statements made in the EBA's June 2019 Opinion, specifically:

Paragraph 19: "*Inherence may include retina and iris scanning, fingerprint scanning, vein recognition, face and hand geometry (identifying the shape of the user's face/hand), voice recognition,* ***keystroke dynamics (identifying a user by the way they type and swipe, sometimes referred to as typing and swiping patterns)****, the angle at which the PSU holds the device and the PSU's heart rate (uniquely identifying the PSU), provided that the implemented approaches provide a 'very low probability of an unauthorised party being authenticated as the payer', in accordance with Article 8 of the RTS on SCA and CSC.*"

Paragraph 20: "*The swiping path memorised by the PSU and performed on a device would not constitute an inherence element, but may rather constitute a knowledge element, something only the user knows.*"

Based on this June 2019 EBA Opinion the minimum viable proposition (MVP) recommended is for issuers to leverage 3DS flows and integrate their chosen behavioural biometric solution via the ACS provider (if applicable). The diagram below illustrates a **possible** technical approach:




This approach will enable customers to authenticate easily using OTP with the behavioural biometric analysis taking place in the background.

Issuers, can, however, work with their ACS and behavioural biometric suppliers to enhance current 3DS flows so that extra customer data (e.g. email address or cardholder name) is captured providing additional data for enhanced behavioural biometric profiling.
Issuers will need to ensure that their final implementation solution complies with all the relevant requirements.

## 2. Password – Knowledge

The usage of password (knowledge) as the second factor over and above OTP is also an SCA compliant alternative. However, this solution is more susceptible to fraud.

Issuers choosing this solution will need to bear in mind that the chosen password type (or other knowledge factors in line with the requirements) does not create risk to customers and/or other payment journeys. In addition, a robust mechanism for password management (i.e. password reset) will need to be put in place to minimise any fraud exposure

## How can e-merchants help?

The recommended position of using behavioural biometrics alongside OTP as the two factors of authentication for (non-app) online transactions avoids the unwelcome prospect of online shoppers requiring a static password or their card PIN, in addition to an OTP. Past experience in the UK and abroad has shown this to be highly disruptive, whilst creating new opportunities for fraud.

Behavioural biometrics solutions will require javascript integration between the ACS and the behavioural biometric solution provider for 3DSecure browser-based authentication challenge flows.

Therefore, merchants are encouraged not to implement restrictions on their websites that could interfere with such scripts. Possible restrictions could be related to the inclusion of third-party content, CORS restrictions, or similar.

Merchants are also encouraged to ensure that when enabling javascripts they do so in a safe manner so as to allow the usage of behavioural biometrics for web browser shopping whilst providing customers with a convenient way of authenticating. This in turn will avoid the unwelcomed need to use other authentication solutions which could add friction to the customer's online check out experience.

## What are the next steps?

UK Finance will be keeping track of industry readiness and will also evaluate the feasibility of coordinating a behavioural biometric supplier/vendor event for issuers that would welcome some extra guidance.

However, issuers are encouraged to take the necessary steps to define their plans to ensure a second factor is added to their OTP solution (if applicable) as soon as possible.

It is each issuer's responsibility to:

- Select their behavioural biometrics provider and coordinate with any other relevant suppliers involved on the delivery of their chosen solution.
- Define the authentication requirements based on the behavioural data provided.
- Ensure that data collected and processed as part of their chosen solution meets the minimum standards set by the EBA and in compliance with the FCA's requirements set out in its Approach Document.
- Identify and address any GDPR and PECR requirements.

The guidance provided does not preclude an issuer's evaluation of alternative authentication solutions under other operating models allowed by the SCA rules, for example, delegated authority.