Strong Customer Authentication communication on authentication methods and vulnerable customers

Date: 16 December 2020

Who is this communication for: UK Finance is providing this guidance to assist card issuers in identifying and assessing solutions for customers for whom the application of SCA may present a number of challenges.

What should you do: Vulnerability is both temporal and personal to the individual – resulting from a range of characteristics which fall into four key groups: health, financial capability, resilience, or life events. Recent global events, particularly coronavirus (Covid-19) may contribute to customers being vulnerable and less able to represent their own interests.

The FCA will shortly be issuing Final Guidance on the Fair treatment of Vulnerable Customers and Card issuers will be required to embed a culture which recognises vulnerability and develops inclusive service propositions and processes which ensure that vulnerable customers are not excluded from performing e-commerce transactions.

Executive Summary

SCA requires authentication of customer-initiated transactions based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something the user possesses) and inherence (something the user is).

Technological advancements are changing the ways in which consumers interact with business across all sectors and the pandemic has accelerated this trend. The move towards digitisation of financial services offers many benefits including: increased access to services at all times of the day or night, lower costs and improved accuracy and efficiency, enhancing customer outcomes, however it is vital to ensure that no one is left behind. Financial and Digital Exclusion are recognised as key drivers of vulnerability and firms need to consider how inclusive design principles can be leveraged to ensure that digital advancements improve access to services for all consumers.

With the introduction of SCA, there is a need for payment service providers to continue to recognise the wide variety of consumers and the ways in which they access goods and services. Whilst the move to digital continues to make advancements, issuers will need to be able to evidence that they have considered what alternative authentication options can be made available to consumers who show characteristics of vulnerability.

Issuers will generally deploy two main options for customers to authenticate, this will include mobile banking solutions and one-time passcodes plus behavioural biometrics and in limited cases, a knowledge factor. Some customers will be unable to authenticate through these more traditional channels and this guidance is to help issuers ensure they consider these customers.

Relevant legislation and FCA Guidance on vulnerable customers

One of the objectives of the Equalities Act 2010 is to bring together all those characteristics in which it is unlawful to discriminate or establish a single approach to discriminate, with some exceptions. The act states people who have a disability or have had a disability in the past must be protected against discrimination. The act provides that an individual has a disability if:

- they have a physical or mental impairment or
- the impairment has a substantial and long-term adverse effect on the person's ability to carry out normal day to day activity.

Due to the range of categories and degrees of impairment, the authentication requirements for SCA could have a detrimental impact on customers with disabilities from performing e-commerce card-not-present transactions. For these reasons, special care should be given to these consumers to ensure they are not excluded. Under the Equality Act 2010, banks must provide customers with access to all their products and services which may require providers to design-in reasonable adjustments.

The desire is that vulnerable customers achieve outcomes as good as all other customers. The FCA has identified 4 key drivers that can increase a vulnerable consumers susceptibility to harm. These include:

Health: health conditions or illnesses that affect the ability to carry out day-to-day tasks including mental health which will be a key consideration during 2021

Life events: major life events such as bereavement, job loss or relationship breakdown

Resilience: low ability to withstand emotional or financial shocks

Capability: low knowledge of financial matters or low confidence in managing money (financial capability). Low capability in other relevant areas such as literacy or digital skills

What Issuers Need to Consider

Card issuers should offer a range of options for customer to authenticate, that will address a proportionate range of vulnerabilities and provide effective safeguards recognising that an individual's vulnerability may increase their risk of becoming a victim of fraud and scams.

The range of options available should enable Card Issuers to meet the needs of the majority of vulnerable customers, however situations may arise where card issuers have exhausted all of their existing solutions and an issuer cannot apply SCA. In these situations, it is UK Finance's view that the issuer may apply one SCA factor where possible. If this is not possible, card issuers are expected to apply some fraud risk mitigation measures (e.g., RBA), monitor the approach, and adjust, as necessary.

There are no applicable exemptions that allow for vulnerabilities and all requirements are subject to audit under article 2, however, for the purposes of inclusion these, may be considered as grounds for adopting a more flexible approach than the RTS expressly permit. In reaching a card issuer's chosen approach it is advisable that firms are able to demonstrate that all possible options have been explored.

The table below expands upon the key drivers and provides illustrative examples of considerations card issuers should make. The table also provides a non-exhaustive list of authentication options for some conditions that customers may have.

Factors to consider	Example Conditions	Examples of authentication options	Comments
Physical disability	Musculoskeletal injuries Amputation Spinal injury	Device binding + facial recognition Device binding + voice recognition Passphrase + device binding	Issuers should consider the severity of conditions and explore options that least impact their customers.
Severe or long-term illness	Cancer Dementia Epilepsy Hypertension and high blood pressure	SMS OPT + Mobile App Dynamic card security code + voice Knowledge, possession, or inherence Knowledge, possession, or inherence	In addition to severity considerations, issuers should also explore whether Lasting Power of Attorney or Court Protection Order is in place / required.
Hearing or visual impairments	Loss of central vision Loss of peripheral vision Blurred vision Partial and total hearing impairment	Device binding + facial recognition Passphrase + fingerprint QR code + voice recognition SMS OTP + Mobile App	Issuers should consider the remote channels their customers are using to perform e-commerce transactions and where possible use the same channels to deliver an authentication challenge e.g., e-com transaction through a mobile phone or possession of the mobile phone and biometrics via a mobile app to authenticate customers. Issuers should also consider a range of other options including email OTP, card readers etc where appropriate.
Poor mental health	Chronic anxiety Neurological condition Schizophrenia	Possession + inherence Possession + inherence Possession + inherence	Knowledge based challenges for this category of customers may not be the most appropriate and issuers may consider a combination of possession and inherence factors in order to support the needs of their customers.
Low mental capacity or cognitive	Anxiety Special educational needs Obsessive compulsive disorder	Possession + inherence Possession + inherence Possession + inherence	As above

Non-exhaustive Authentication Options

In June 2019, the EBA published further guidance on SCA requirements and, in particular, what may constitute a compliant element in each of three possible categories.

Knowledge:

- Password
- PIN
- Knowledge-based challenge questions
- Passphrase
- Memorised swiping path

Possession:

- Possession of a device evidenced by an OTP generated by, or received on a device
- Possession of a device evidenced by a signature generated by a device
- Card or device evidenced by QR code scanned from an external device
- App or browser with possession evidenced by device binding
- Card evidenced by a card reader
- Card with possession evidenced by a dynamic card security code

Inherence:

- Fingerprint scanning
- Voice recognition
- Vein recognition
- Hand & face geometry
- Retina & iris scanning
- Keystroke dynamics
- Angle at which device is held

In addition to the above, there are some points to note.

Assistive Technology

For people with learning disabilities, ecommerce provides a way to cope with cognitive, physical, and emotional limitations by shopping within a controlled, stress-free environment. For some people with learning disabilities, navigating a densely populated product page or remembering the steps in the purchase process may not be easy. Having tools that can help organise tasks, aid memory, maintain focus, or improve comprehension can improve their experience with online shopping. Card issuers are asked to maximise the use of assistive technology and communicate options to cardholders to further reduce friction in a customer journey.

E.g., Visual Impairment

Screen readers are a type of computer software that translates on-screen text into an audio voice or into braille for refreshable braille displays. The voice speed is adjustable, giving users more flexibility to follow along at a comfortable pace. To keep users oriented, screen readers read aloud specific graphic elements like icons, images, or sections like “payment options”. The software identifies these sections as a user highlights them with their mouse or hovers over them with their cursor. The software will also read back any text the user inputs, like their name or credit/debit card number.

Online Resources:
ChromeVox or Talking Web — Text-to-talk Chrome extensions
Firefox browser — Compatible screen reader
Best screen reader — web browser pairings
Free screen readers - NVDA, Serotek, Apple Voice Over, ORCA, BRLTTY, Emacspeak, WebAnywhere, Spoken Web, ChromeVis

Amazon's screen reader optimized website.

Software:
JAWS (Windows)
VoiceOver — Screen reader and media creation tool (Mac)
NVDA — Free screen reader (Windows)
BRLTTY — Driver for braille displays (Linux).

Chip and signature:

In the context of face-to-face transactions, chip and paper-based signature is not an alternative to Chip & PIN for the purposes of SCA and should only be used for financial inclusion purposes for people who have difficulty remembering or entering in a PIN. This is required in order to allow for compliance with the Equality Act (to ensure customers with a disability are not discriminated against). Card terminals in shops are designed to automatically prompt shop staff to ask for a signature when one is needed.

Session time out:

In the context of online banking, UK Finance is of the view that there are circumstances where allowing longer than the 5 minutes time out required by Article 4(3)(d) could be reasonably justified in an online banking context:

(a) vulnerable customers may need a longer session time, likewise others for financial inclusion purposes, and a longer time out period would be a reasonable adjustment under the Equality Act

(b) corporate customers often require extended sessions to effectively manage and administer their corporate accounts

(c) customers generally need sufficient time for customers to read longer documents such as terms and conditions. The RTS do not provide for any exceptions and all of the requirements are subject to audit under Article 2, however UK Finance considers these to be good reasons for adopting a more flexible approach than the RTS expressly permits.

Email OTP

UK Finance note that there is nothing in the RTS nor the EBA opinions to preclude the use of other means of sending OTPs other than SMS, namely landline or email, as a compliant SCA possession factor, provided that they can be associated, bound or linked adequately to the particular cardholder and provided the requirements of Article 7 of the RTS are met.

In the context of vulnerable customers and issuers seeking to maximise a customer's ability to authenticate, there could be reasonable justification to use Email OTP as one of a number of authentication options.

Customers Unable to Authenticate through SMS OTP or Mobile App:

UK Finance notes that customers unable to use authentication methods such as SMS OTP or Mobile App do not meet the definition of vulnerability in the context of this guidance. Card issuers are specifically asked to provide suitable alternative authentication options that enable customers to authenticate. The FCA require issuers to make them aware of alternative options that they will make available to this category of customers.