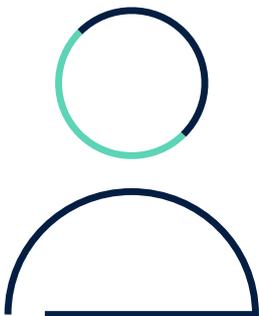


STRONG CUSTOMER AUTHENTICATION: COMMUNICATIONS FOR CONSUMERS

May 2019

WHAT IS STRONG CUSTOMER AUTHENTICATION (SCA), AND WHY IS IT BEING INTRODUCED?



Strong Customer Authentication (SCA) is a new set of rules that will change how you confirm your identity when making purchases online.

Next time you shop or bank online, you may need to undertake an extra step to confirm it's really you. This could mean your bank or provider using a number of ways to verify a purchase or login such as a passcode via text message, receiving a phone call to your landline, a card reader or using an app on your smartphone.

SCA is being introduced to help further reduce fraud. With increasing amounts of purchases being made online, these new rules will provide the extra protections necessary to ensure that customers are safe when purchasing online and their money is better protected.

KEY MESSAGES



- In order to shop online or do online banking, you may be asked to take extra steps to confirm it's really you.
- This is due to new rules that are being introduced, changing how you prove your identity online. These rules will further help to reduce fraud and protect customers.
- You need to be ready to provide an extra step to verify yourself, if required. This could mean your bank or provider using a number of verification methods such as a passcode via text message, receiving a phone call to your landline, a card reader or using an app on your smartphone.
- Some types of transactions are exempt from strong customer authentication, meaning that you may not always be asked to complete extra security steps.
- You need to make sure your bank or provider has up to date contact details for you (such as a telephone number and email address).
- You can contact your bank or provider for more information on these changes, including how you may need to confirm your identity.
- Remember: A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out personal or financial details to use a service that you're expecting to contact you, that you've given your consent to and that you trust.

WHAT WILL SCA MEAN FOR ME?



These rules will apply to you when you're making an online purchase or banking online. When buying items from online retailers, you may receive a text message from your bank or provider containing a passcode. You will then be prompted to enter this code on screen before your payment will be taken.

Your bank or provider should also offer alternative ways of confirming who you are. These can include a call to your landline phone, a card reader,

or using your banking app on your smartphone, if you have one.

When using online banking, you will be asked to verify who you are in a similar way as for online shopping. If you bank via an app you may have already provided the authentication needed by using your fingerprint, a code, or facial recognition to log in.

You may not be asked to prove your identity in this way for every purchase or transaction.

WHAT DO I NEED TO DO?



Be ready for the changes by making sure your contact details are correct and up to date. If you bank online, you may be able to update your phone number and other details there. If not, speak to your bank or provider directly by visiting your branch or giving them a call.

As always, remember to Take Five and stop to think. A genuine bank or organisation will never contact you out of the blue to ask for your PIN, full password or to move money to another account. Only give out your personal or financial details to use a service that you have given your consent to, that you trust and that you are expecting to be contacted by.

FAQs

I don't have a mobile phone. How can I verify my identity?

Your bank will offer appropriate arrangements to help you verify your identity. This could mean your bank or provider using a number of other verification methods such as receiving a phone call to your landline or a card reader. Please contact your bank or provider to update your details and to discuss other options.

Do these rules only apply to online purchases?

Whilst the biggest changes you're likely to see are online, SCA will also apply in a face to face environment. As Chip & PIN is a familiar way of proving your identity, for most purchases you won't have to do anything different. However, if you make contactless payments, SCA may mean you have to input your PIN slightly more often.

These rules don't apply to travel, so your regular contactless payments for the bus, train or tube won't be affected.

I buy online from the same websites regularly. Will I have to prove my ID every time?

In future, you may have the opportunity to add some sellers to a 'trusted beneficiary' list, meaning that you will not need to go through SCA when purchasing from that store or organisation. However, if your bank or provider suspects unauthorised activity (such as an unusually large order or delivery to a different address) they may still ask you to confirm your identity. Please note that the implementation date for this feature will vary, depending on your bank or provider and the merchants involved.

Why is my bank/provider making it harder for me to shop online?

SCA is being introduced to help further reduce fraud. With an increasing number of purchases being made online, extra protections are necessary to ensure that customers are safer, and their money better protected.

Is every payment I make going to be affected?

Not all payments will be affected. Non-electronic payments, such as cash and cheques, are not in scope of these changes. All purchases made by telephone (for example, buying from a catalogue by calling the company and giving your details over the phone) are not in scope.

Automatic payments that you make regularly to the same provider (e.g. a subscription to online streaming platform) do not require SCA. You may still be asked for additional identity checks when initially setting up these payments.

Low value payments (under £30), including those made on contactless cards, do not always require strong authentication. However, if you have made multiple payments within a short period of time, you may be asked to authenticate. For contactless, this will mean entering your PIN.

Background/Further Information

1. The EU's revised Payment Services Directive (PSD2) will make strong customer authentication for all payment providers a legal requirement from 14 September 2019. Some payment providers already widely use multifactor or two-factor customer authentication for online transactions, while others will be implementing the changes ahead of September's deadline. PSD2 is part of UK law and as such implementation is not dependent on the outcome of the ongoing Brexit negotiations.
2. Payment providers are aware of the limitations of some forms of verification, for example those with poor sight or that don't have access to a mobile phone. We therefore expect that providers will have appropriate solutions in place to allow their customers to authenticate themselves. This could mean your bank or provider using a number of verification methods including, for example, a phone call, text, banking app and/or card readers to check your identity.
3. There are a number of exemptions from SCA for low-value and low-risk transactions. This includes an exemption for low-value transactions of under £30. Multifactor authentication will still be required once a customer's total payments exceed a cumulative value of £90 or when five payments of up to £30 have been made.