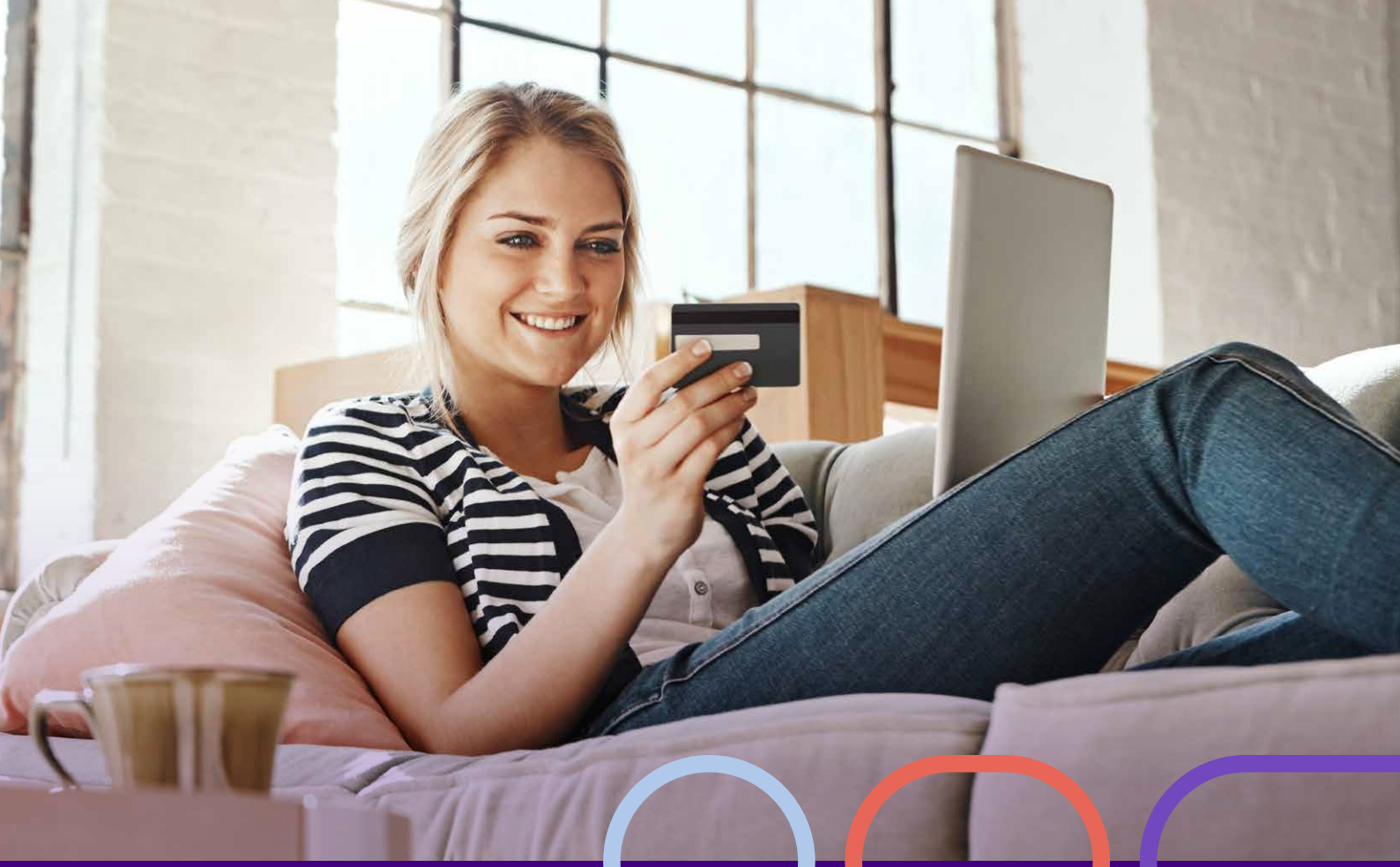


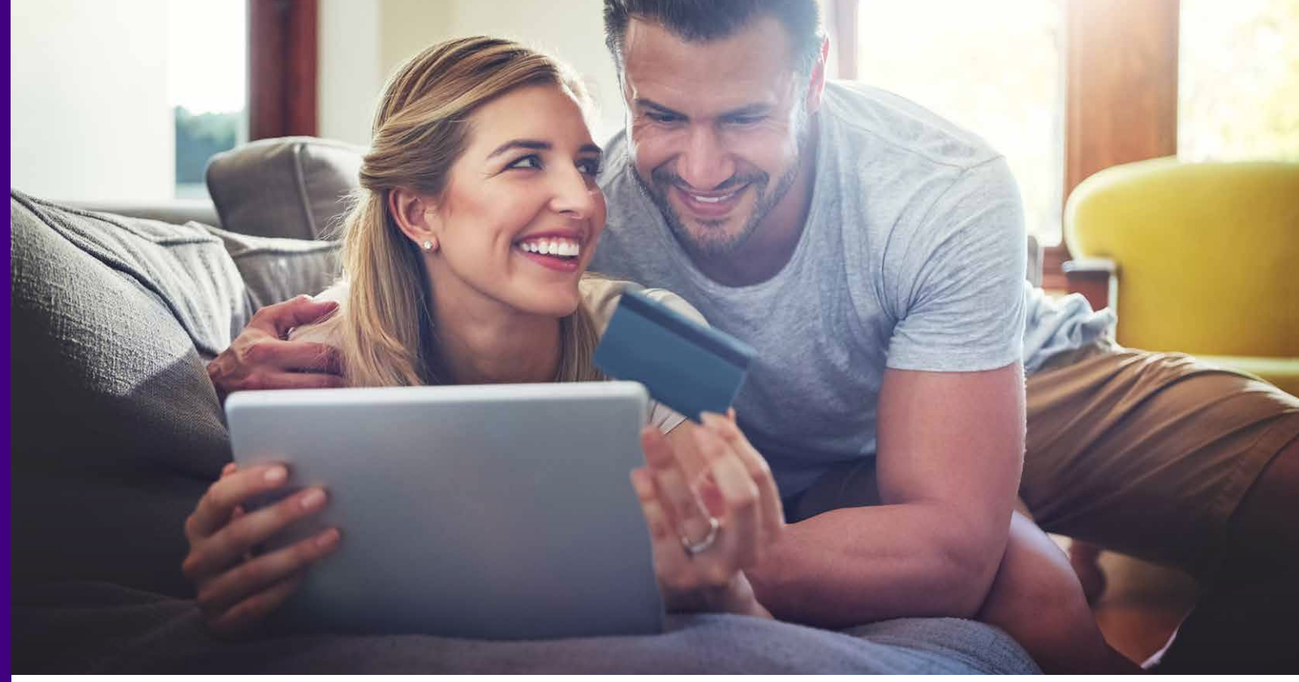
A simple guide to SCA

What is Strong Customer Authentication (SCA) legislation? Information for online businesses

Cashflows

Legislation changes can be a challenge, especially when the directions are full of complex clauses and jargon.

The second Payment Services Directive (PSD2) is no different. Part of that is Strong Customer Authentication (SCA).



We're going to explain the key terminology used around SCA, answer some of your immediate questions while preparing your business, and suggest some actions that will help get you ready.

What changed?

PSD2 came into force at the start of 2018, and required changes to be made across the payments industry.

One of the bigger changes was the introduction of SCA, which became law in Europe on the 1st of January 2021, enforced by the European Banking Authority. In the UK, the ramp-up began from June 2021 with full enforcement of the deadline by the Financial Conduct Authority (FCA) starting from March 2022.

What is Customer Authentication and why do we need it?

Authentication happens when a customer proves they are who they claim to be, by providing additional data at checkout – such as a PIN, thumbprint or password.

This is most commonly seen online with 3-D Secure, an authentication tool developed by Visa and Mastercard to provide an additional security layer for online transactions. 3-D Secure adds an extra step in the online transaction process, where a customer must enter a password or PIN to prove that it's them making the payment.

But what exactly does 'Strong' mean?

There could understandably be some confusion around exactly what counts as 'Strong', in authentication terms.

The card schemes and regulators have agreed that 'Strong' means Two-Factor Authentication. Good, all clear then.

3-D Secure adds an extra step in the online transaction process, where a customer must enter a password or PIN to prove that it's them making the payment.

Wait, what is two-factor authentication?

Here's where it gets interesting. 'Two-factor' means that a combination of two security elements is used to verify the user's identity. This means that users need to complete an additional, second step to verify themselves.

To qualify as 'Strong' the two factors need to be a combination of verifiers, using:

- Something the card holder knows, such as password or PIN
- Something they own such as a mobile phone
- Something they are, such as a fingerprint or face recognition.

For example, asking a card holder to enter a code sent to their mobile phone verifies them using something they own. This means the card holder is far more likely to be who they say they are, which will reduce online fraud and increase card security.

With SCA in force, two-step authentication needs to happen at checkout for online purchases.

3-D Secure Version 2.0 or later provides the additional authentication factors needed to meet this requirement.

OK, what can be done about it?

The good news is, online businesses don't need to solve this problem themselves, as 3-D Secure Version 2.0 (or later) meets this requirement.

But complying to this change is key to keeping customers safe.

In preparing for these new laws, Visa and Mastercard developed enhancements to their 3-D Secure verification tool, releasing 3-D Secure Version 2.0 in 2019 (also known as EMV 3-D Secure). They recommended that businesses start using it as soon as possible, in order to be ready for when the law was enforced.

Visa estimates that just over half of all transactions fall in scope for SCA and therefore require 3-D Secure (V2.0 or later) authentication at checkout.

It's important that your website has activated 3-D Secure Version 2 (or later) for relevant transactions.

How does this affect my online business?

There is no doubt that 3-D Secure Version 2 affects online businesses. First, it reduces fraud and increases security for your customers, leading to fewer chargebacks as a result.

But it does also increase friction in the checkout experience for larger purchases, which could impact your conversions. 3-D Secure Version 2 has been built with this in mind.

And considering most of your competitors will be in the same boat, the real loss of this is minimal.

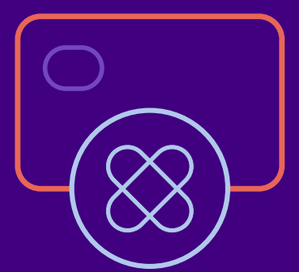
Which transactions are in scope for SCA?

The requirement applies to all ‘card holder initiated’ transactions, so certain transactions fall out of scope.

Telephone and mail order payments are not subject to SCA, and recurring payments also fall out of scope.

Transactions using EU issued cards and under €30 in value are also exempt. These exemptions reduce payments friction.

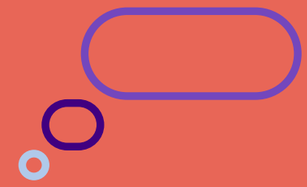
Not implementing 3-D Secure Version 2 is not an option as, since 2021, banks and issuers have been declining non-compliant transactions.



What can I do to ensure my payments remain seamless?

If you're an online business and are worried you're being impacted by the updated 3-D Secure Version 2, contact your payments partner or payment gateway to find out what you can do - you may need to make changes on your website or change your security settings to enable correct transaction flagging and implement exemptions that should boost conversions.

If you're working with Cashflows, you can email us at **sca@cashflows.com**.



Interested to work with us?

hello@cashflows.com

Cashflows