

# A simple guide to SCA

Preparing for Strong Customer  
Authentication (SCA) legislation:  
Information for online businesses

Cashflows

Preparing for 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's happening?

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

One of the bigger changes is the introduction of SCA which became law in Europe from 1 of January 2021, enforced by the European Banking Authority. In the UK, the ramp-up begins from June 2021 with full enforcement deadline by the Financial Conduct Authority (FCA) 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. Now users need to complete an additional, second step to verify themselves.

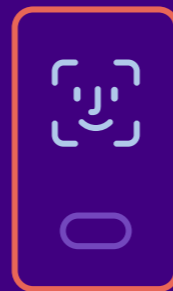
To qualify as 'Strong' the two factors need to be a combination of verifiers, using:

- 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.

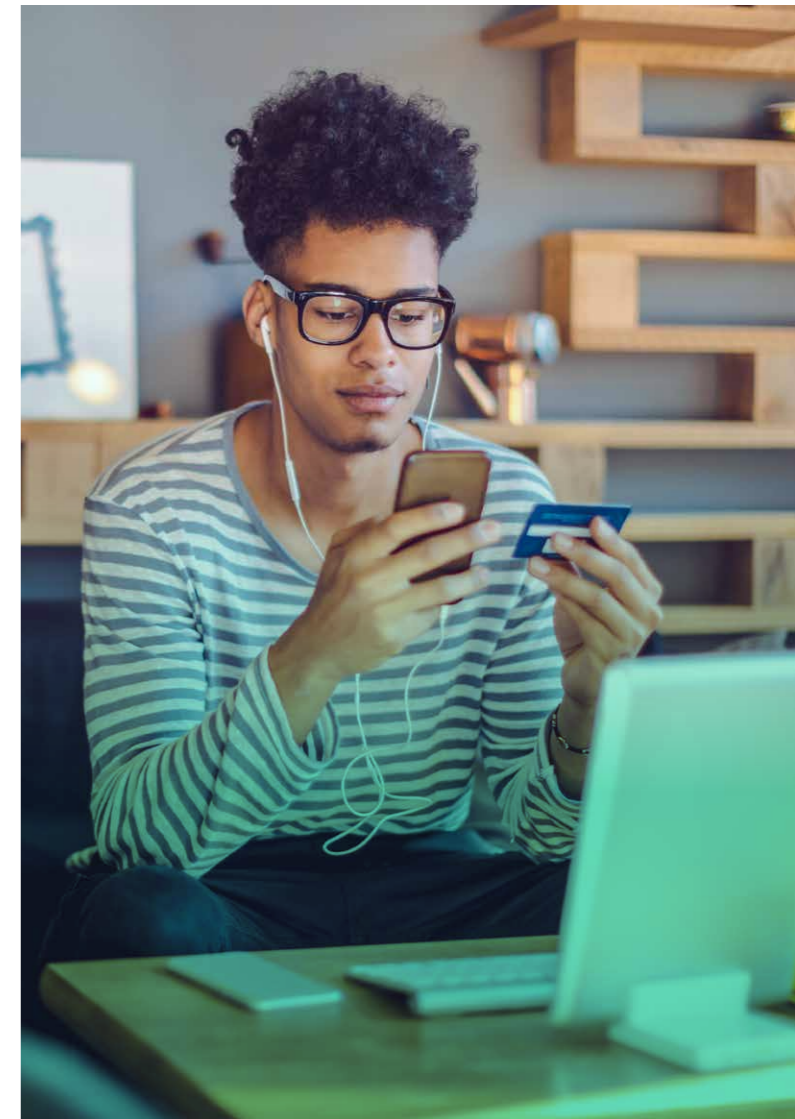
**The regulators have confirmed that 3-D Secure Version 2.0 or later provides the additional authentication factors needed to meet this requirement.**



# OK, what can be done about it?

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

But you do need to take action if you haven't already.



In preparing for these new laws, Visa and Mastercard have 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), and strongly recommend businesses use this in order to be ready for the law to be enforced.

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

It's important that your website is set up to activate 3-D Secure Version 2 (or later) for relevant transactions.



## How will this affect my online business?

There is no doubt that the change will affect online businesses. First, it will reduce fraud and increase security for your customers and it's likely you will see fewer chargebacks as a result.

But it's also likely to 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 likely to be minimal.

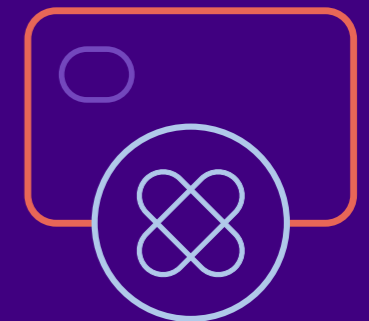
## Which transactions are in scope for SCA?

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. You'll find more detail on out of scope and exempt transactions in our [PSD2 Whitepaper](#).

Not implementing 3-D Secure Version 2 is likely to have an impact on your business when banks and issuers start declining non-compliant transactions in 2021.



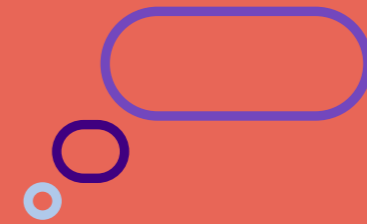
# What if I'm not ready, what will the impact be?

While the future is difficult to predict, its expected that you will start to see more declines from issuers through the ramp-up, as authorisation processes are changed. Any event, in scope transactions that don't fulfill the SCA requirements after the deadline are likely to be declined.

While the FCA's deadline is now March 2022, Visa and Mastercard recommend that all card accepting merchants be ready before that. You may not feel the impact immediately, but it could affect your sales and it's worth being prepared.

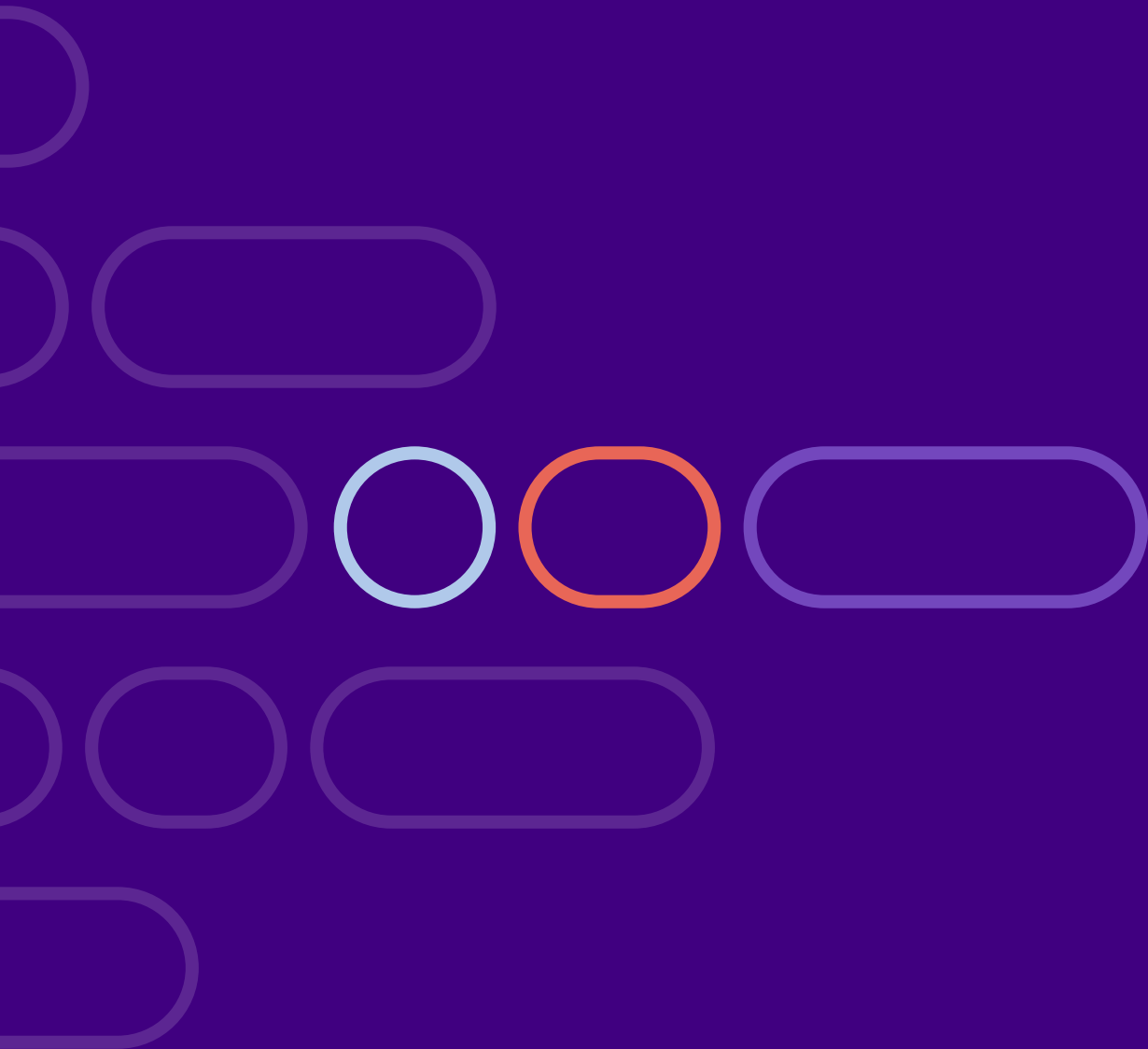
# What can I do to get ready?

If you're an online business and are worried you'll be impacted, contact your payments partner or payment gateway to find out what you need to do - you may need to make changes on your website or change your security settings. If you're working with Cashflows you can email us at [sca@cashflows.com](mailto:sca@cashflows.com).



Interested to work with us?

[hello@cashflows.com](mailto:hello@cashflows.com)



Cashflows