judo®

An introduction to Strong Customer Authentication (SCA)

Updated April 2022

Contents

3 Foreword: The road to SCA
4 What is SCA?
6 Why was SCA enforced?
7 How does SCA work?
8 Your customers and SCA
10 Are there any exemptions to SCA?
11 What impact does SCA have on your business?
14 What is 3DS2 and how does it work?
15 Summary: 3DS1 v 3DS2

The road to SCA.

In 1979, something monumental occurred when Visa introduced a point-of-sale terminal to merchants. For the first time, consumers could choose to spend directly from their bank accounts via a single plastic card rather than being limited to the cash in their wallet.

A tremendous shift in the way merchants and consumers could exchange goods and services, this card payment experience would remain virtually unchanged for the next quarter of a century.

Then in 2006, Chip & PIN was formally adopted to combat fraud on lost, stolen and counterfeit cards. From 14 February, all card transactions would require customers to enter their PIN at the checkout.

Described as the "largest change in the way we pay since decimalisation", Chip & PIN marked the end of the customer signature and sparked a rapid succession of digital payment innovations. In 2007, the first contactless credit cards were issued by Barclaycard in the UK. Contactless debit cards would follow just two years later.

Ahead of its time, contactless would not take off as a serious payment method in the UK until 2012, when NFC technology became more readily available to merchants. Apple Pay, Samsung Pay and Google Pay would then arrive in quick succession over the next three years.

It legitamised contactless and mobile payments in the eyes of merchants and consumers alike, as well as helping to solve the experience gap between in-store and online shopping, these innovations confirmed the now unrivalled position of digital payments.

However, this shift towards a more convenient and frictionless payment experience, where consent and acceptance became an instant tap or click, inevitably created more risk and fraud potential, both for merchants and their customers.

Identifying the accelerating changes to how digital payments are now made and accepted, in 2013 the European Commission sought to reinforce payment security and consumer protection, part of an initiative that would come to be known as Payment Services Directive Two (PSD2).

Born out of PSD2, the term Strong Customer Authentication (SCA) came to everyone's attention. In short, SCA is a new set of legal payment requirements that consist of additional security steps that need to take place when a customer makes certain purchases.

SCA affects virtually every EU merchant selling online. The EU required relevant businesses to have a fully compliant SCA strategy in place by 31 December 2020. While the UK's Financial Conduct Authority (FCA) had an extended deadline 'til the 14 March 2022, some UK issuers began randomly checking if transactions were SCA compliant from 1 June 2021.

This guide will take you through everything you need to know about SCA, how it affects your business, the steps that need to be taken, and what Judopay can do to help ensure you have a fully compliant strategy in place.

Jeremy Nicholds, CEO
Judopay

What is SCA?

Strong Customer Authentication (SCA) is an EU and UK legal requirement for online payments that's already in force in most of Europe and came into force in the UK on 14 March 2022.

As consumers purchase more goods and services online, the need to authenticate identity during transactions has become essential in making payments more secure and reducing cases of fraud.

In the past, shoppers have only been required to enter their financial details to complete an online purchase.

The new SCA regulation now insists that merchants include an extra layer of ID security when their customers make an online payment

£671.4m

fraud losses on UK-issued cards in 2018.

UK Finance

13%

estimated percentage of transactions that could be abandoned in 2020 without the right SCA technology.

British Retail Consortium

300m

number of people in Europe who will need to change the way they buy.

Small Businesses

75%

of merchants are unaware of SCA.

UK Finance

The FCA has been working with the industry to put in place stronger means of ensuring that anyone seeking to make payments is not a fraudster. While these measures will reduce fraud, we also want to make sure that they won't cause material disruption to consumers themselves; so we have agreed a phased plan for their timely introduction.

Small Businesses

Why was SCA enforced?

December 2007

The first Payments Service Directive (PSD1) is introduced by the EU. Part of its aim is to create more competition within the payments industry by allowing non-bank companies (fintechs) to carry out financial transactions for the first time.

November 2009

PSD1 becomes UK law, as part of the 2009 Payment Services Regulations. New fintech payment services begin to emerge that compete to deliver better, faster and more secure payment services to merchants and consumers.

November 2015

The second Payments Service Directive (PSD2) is passed by the EU. It recognises that new payment services are now facilitating consumers' electronic payments and aims to further enhance data protection and reduce risk. The concept of Strong Customer Authentication (SCA) is identified as a solution to significantly boost security around online payments.

January 2019

PSD2 enters into force and EU member states are instructed to implement the directive into domestic law. The deadline for implementing SCA is set at 14 September 2019. From this point, all online payments will require additional authentication, with some exemptions (more on this later).

September 2019

SCA requirements officially go into effect, but an earlier announcement from the European Banking Authority (EBA) leads to the enforcement deadline being extended to: 31 December for EU members.

May 2020

Following an earlier decision to extend the UK deadline to 14 March 2021, the Financial Conduct Authority (FCA) takes into account the impact of the COVID-19 pandemic and further extends its enforcement date to: 14 March 2022.

How does SCA work?

From **14 March 2022**, SCA became mandatory for most online UK transactions (excluding SCA exemptions) and became mandatory across most of Europe in December 2020. Many consumers will experience a standard payment flow. However, if an Issuer challenges the transaction (i.e. requires more data to confirm the cardholder is the person making the transaction) the consumer will be asked to provide a combination of two of the following authentication factors:

Something you **are.**

(e.g. Fingerprint, face recognition, voice pattern).

Something you **know.**

(e.g. PIN, password, passphrase, secret fact, sequence).

Something you **have.**

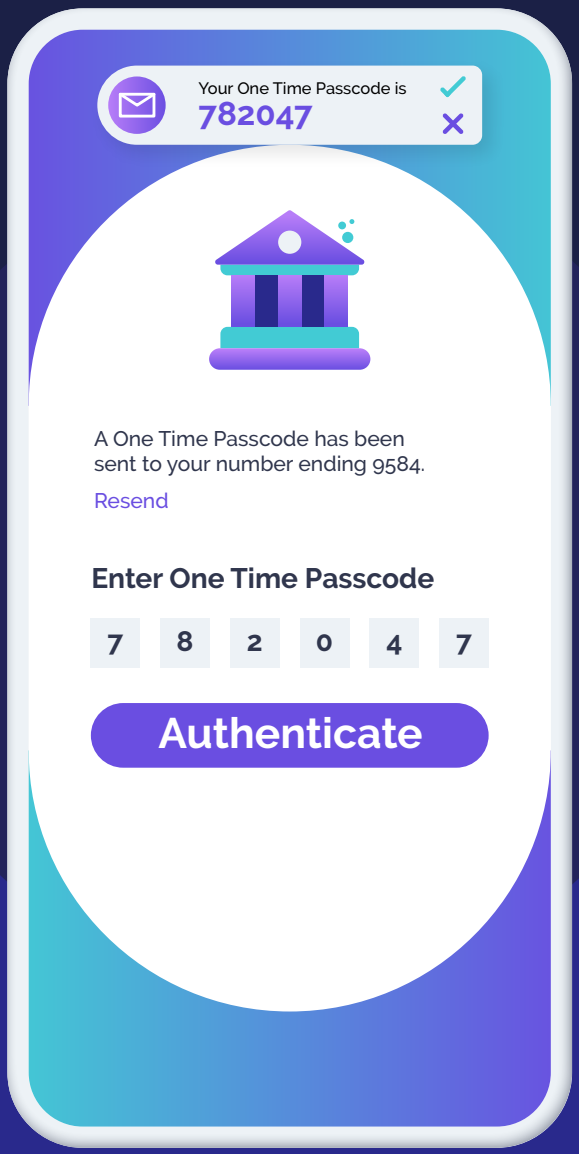
(e.g. Card, smartphone, wearable device).

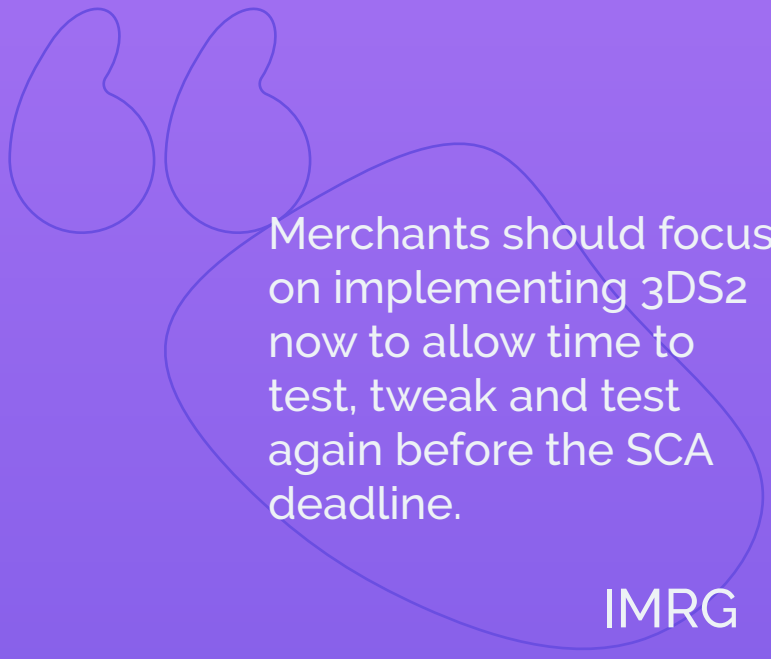
Your customers and SCA.

Many of your customers will already be familiar with two-factor authentication (even if they don't know the terminology).

As an example:

When a customer is asked to enter a one-time code sent to their smartphone (something they **HAVE**) after they've entered their password (something they **KNOW**) to access online banking.





Merchants should focus on implementing 3DS2 now to allow time to test, tweak and test again before the SCA deadline.

IMRG

Are there any exemptions to SCA?

Yes, all merchants taking online payments need to comply with SCA, but there are exemptions that will apply to some businesses:

Low-value payments under £45 (or €50)

• This follows a decision to increase the contactless limit from £30 as a response to COVID-19 (since 1 April 2020).
• This exemption takes place until a customer makes more than five exempt payments in a row, although this may change as a result of increasing the contactless limit.

'Whitelisted' eCommerce websites

• Customers will be able to select online shopping sites they trust and regularly use, which means SCA will only be required when they make a first purchase.

Recurring Payments / Merchant-Initiated Transactions (MIT)

• i.e. If your customer takes out a subscription they will only need to prove their identity when they first sign up to your service.

Mail Orders and Telephone Orders (MOTO)

• All transactions that take place via mail or telephone are exempt, as they are not classed as 'electronic' payments.

Low Risk Payments / Transaction Risk Analysis (TRA)

• Certain transactions can be exempt from SCA, provided they are considered low risk and below target fraud thresholds. This must identify unusual changes to a customer's behaviour and work in real-time to ensure a seamless checkout process.
• Checks can include transaction history, location at the time of payment and previous use of a customer's payment device. You can find out more about how TRA works from your payment service provider.

Direct Debits

• e.g. Monthly bills

What impact does SCA have on your business?

1 You will need to ensure your 3D Secure protocol is up-to-date.

The 3D Secure 1.0 (3DS1) protocol (think Verified by Visa, Mastercard SecureCode or Amex's SafeKey) was first implemented in 2001 to verify customer identity and authorise card-not-present payments online.

Virtually outdated before it arrived, 3DS1 remained unchanged for nearly two decades, coming into existence six years before the first iPhone was introduced.

3DS1 usually requires a distracting pop-up window or redirect, is incompatible with any mobile-led shopping experiences, and fosters high levels of basket abandonment.

3D Secure 2.0 (3DS2), an updated version created by EMVCo in 2015, has replaced passwords and PINS with tokenized, biometric and two-factor authentication to help reduce friction during the online payment process, whilst being fully SCA compliant.

2 Your payment flow will become smoother for customers.

While 3DS1 created multiple friction points, like pop-ups, redirects, password requirements or SMS verification, 3DS2 makes it more likely that customers will be able to automatically authenticate their identity without challenge during the online payment process.

3DS2 has seen cart abandoment fall by 70%, while transaction time has been reduced by 80%.

Frictionless Experience with Verified by Visa, Visa, 2018

3 Fraud liability shifted from merchant to issuer/cardholder (in most cases).

To incentivise merchants to adopt 3DS2, merchants will continue to have the liability shift for fraudulent transactions, unless an exemption has been applied* (note - liability shift is also available for fraudulent chargebacks on 3DS1).

Where merchants would usually refund losses incurred by fraud, 3DS2 enables issuing banks to better authenticate the identity of customers during online transactions, reducing fraud disputes and, therefore, lowering the costs associated with chargebacks.

**Note: The 3DS2 liability shift only takes place if two-factor authentication was successful at the online checkout, and a chargeback due to fraud then took place. If two-factor authentication fails or an error occurs, chargeback liability remains with the merchant.*

€50 billion

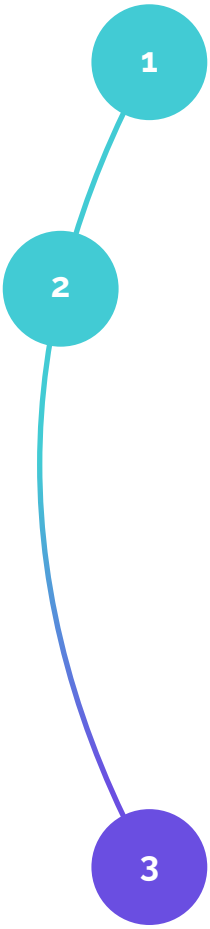
that's what 13% basket abandonment looks like in lost sales volume.

British Retail Consortium

> More than 75% of merchants are unaware of SCA requirements and less than 5% of merchants are currently using 3D Secure 2.1 - the technology required for applying SCA.
>
> UK Finance

What is 3DS2 and how does it work?

While SCA is the legal requirement, 3DS2 is an SCA compliant authentication service. 3DS2 is what adds an extra layer of security to the payment flow to make them SCA compliant. In most cases this will remain a seamless experience, but if the issuer isn't completely satisfied that the real cardholder is the one making the purchase, they'll ask for some additional input to authenticate the transaction.



Customer initiates payment.

Customer enters their card details on your checkout page to start the payment.

Authentication check.

Judopay's 3DS2 solution checks if authentication is required. Depending on the issuer's requirements, we'll share data such as shipping address, customer location or device ID to assure them that the real cardholder is making the purchase.

Option 1: If the issuer is satisfied they'll authenticate the payment.

Option 2: If the issuer isn't satisfied with the ID and risk credentials, the customer will be asked for some additional input to authorise the payment (something they KNOW, HAVE, ARE).

Payment authorised.

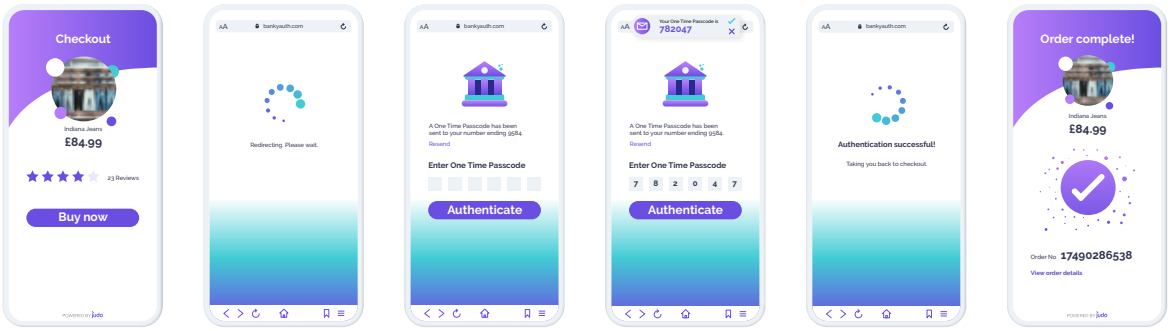
Once the issuer is satisfied that the real cardholder is the one making the payment, the payment can be completed.

Summary: 3DS1 vs 3DS2.

Your customers may recognise the 3DS1 payment flow as an occasional redirect when buying online. 3DS2 is the latest version of 3DS with some key differences including: being mobile optimised, offering exemptions for certain payments and removing the need to redirect customers, which often results in basket abandonment.

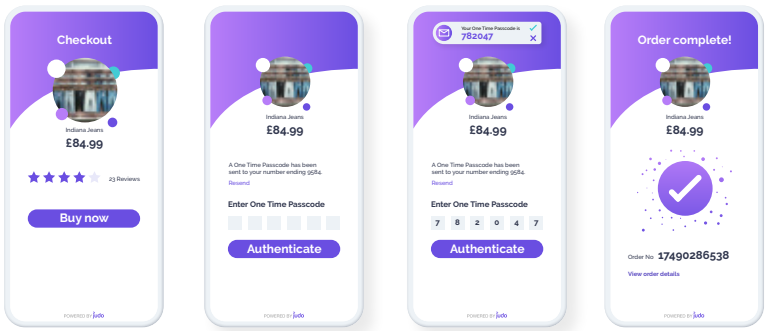
3DS1 flow.

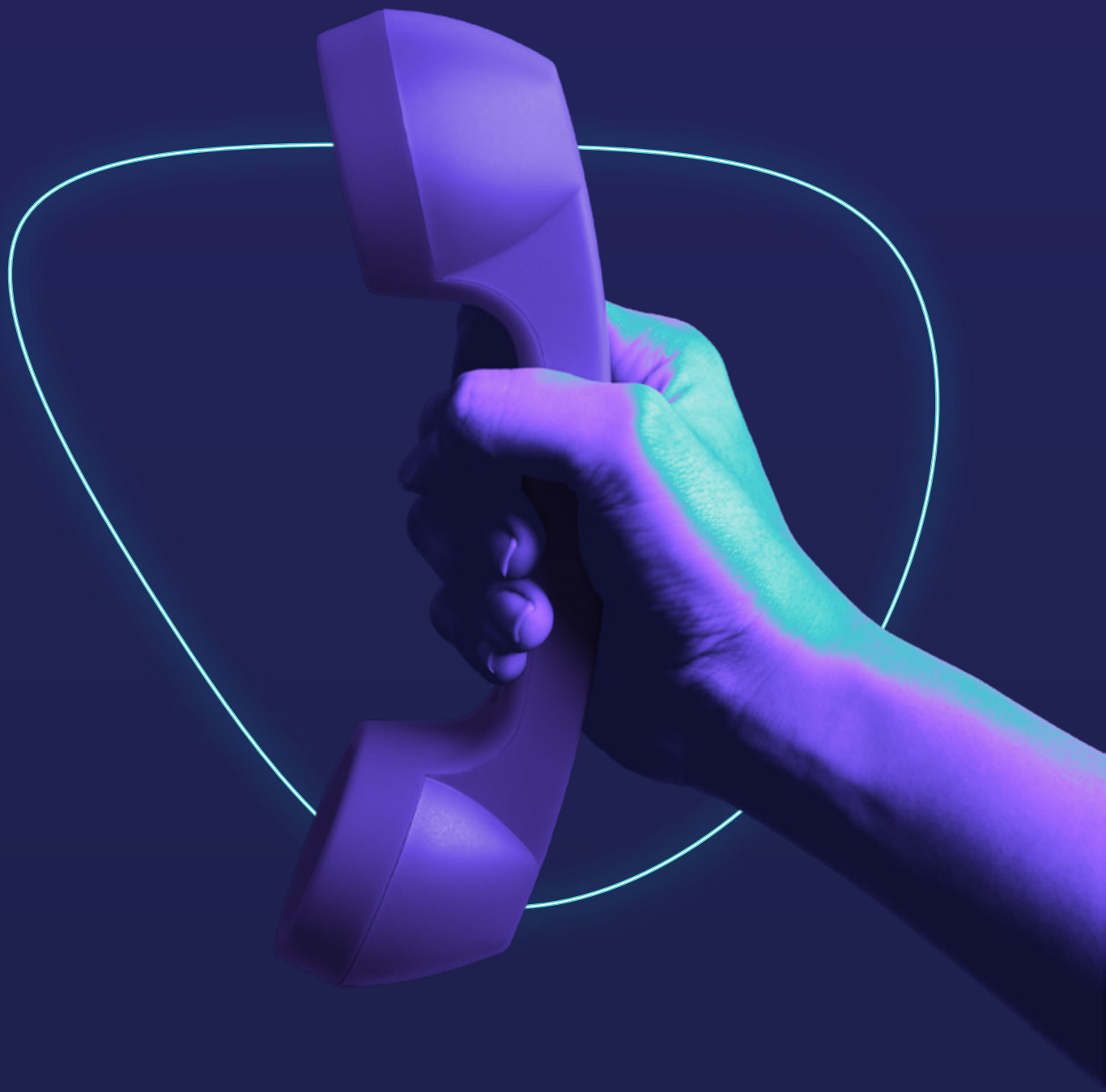
Old payment flow with redirect.



3DS2 flow.

Updated payment flow.





To discuss how Judopay can support your SCA journey, get in touch at:

sales@judopay.com

+44 (0)20 3510 5111

judo®