Cashflows

Maximising Payment Success

PSD2 – Strong Customer Authentication

CF144 1020

Purpose and Disclaimer

Cashflows Europe Limited ("Cashflows") is providing this guide as an overview of the upcoming requirements under the revised Payment Services Directive (PSD2) and the accompanying Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA).

This guidance is provided for general information purposes only and does not constitute legal advice. Cashflows will not accept any liability to any third party in relation to the contents of this document.

Any opinions expressed in this document are the opinions of Cashflows only and may not entirely reflect the views or advice of the Financial Conduct Authority (FCA) and/or European Banking Authority (EBA).

We also expect national competent authorities, such as the FCA and the EBA to provide further guidance, this information is publicly available to anyone who wishes to review it.

Introduction

The Payments industry continues to experience change, and in 2020 the impact of technology continued to increase. New figures show that debit card payments have overtaken cash use for the first time as contactless technology takes a firm hold on day-to-day spending.

Whilst payment speed and convenience is welcomed by consumers, these factors have also raised certain risks as more individuals than ever are being targeted and falling victim to fraud and cybercrime.

PSD2 is certainly driving innovation and transparency in the payments space. The regulation introduces the requirement to ensure that all electronic payments, with a few exceptions, are subjected to SCA.

About Us

Cashflows has been offering merchant account services to customers across the European Economic Area (EEA) since 2010.

We became one of the first independent UK payments institutions to be accepted as a principal member of both Visa and Mastercard. Since its inception, Cashflows has invested heavily in its infrastructure to deliver an industry-leading payments platform. Our cloudbased solution is highly cost-effective, fast, scalable and secure.

Cashflows aims to maximise payment acceptance for our customers and partners through more right-first- time sales, fewer declines and disputed transactions. We do this through a combination of our purpose-built technology, innovation and expertise. The new PSD2 regulations are no different, we aim to be at the forefront of the industry and be amongst the first to extend SCA support to all our merchants.

Contents

Let’s discuss PSD2 4

What is SCA? 5

What is 3D-Secure? 6-7

SCA Exemptions 8

How will you be affected? 9-10

What’s the future holding? 10

Let’s discuss PSD2

Payment Services Directive (PSD2)

PSD2 is a revised version of PSD1, an EU directive administered by the European commission intended to regulate payment services and its providers throughout the European Union (EU) and the EEA which affects banks, building societies, payment institutions, e-money institutions and their customers.

In 2015, the European Parliament accepted a proposal to create safer and more innovative European payment services as well as levelling the playing field for payment service providers. The new rules aim to better protect online payments for consumers and businesses, promote the development and use of innovative online and mobile payments and make cross-border European payment services safer.

With the introduction of PSD2 SCA and the European enforcement of two-factor authentication from 31 December.

A change in the payments

Security
lower risk and reduced fraud. Currently, card-not-present transactions represent around 66% of fraud cases in the payments industry. As such, it is a logical next step to implement new and innovative security measures to tackle this type of fraud.

Online impact
technology is a pervasive influence in many people’s lives and as a consequence, there is a demand for increased levels of security. Up to 49% of organisations admit to becoming victims of fraud and economic crime. This figure has risen by 36% since 2016.

Authentication
introduction of sca criteria includes mandatory two-factor authentication requirement, dynamic linking and enhanced consumer protection.

Implementation
staying compliant with PSD2 regulation requires organisations to review their processes and act proactively to integration changes & technology offerings.

Consumer rights
PSD2 provides enhanced protection for consumers. It introduces greater transparency in electronic payments, new rules for surcharges and currency conversion, and the manner in which complaints are handled.

Sources:
https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html
https://complyadvantage.com/knowledgebase/regulation/psd2-payment-services-directive-2/

What is SCA?

When the SCA requirement is enforced, it is estimated that 9 out of 10 of electronic payments will require the application of SCA, except for those deemed out of scope, or where an allowed exemption is applied to a qualifying transaction.

SCA is applicable to transactions in the EEA only, where both the payer and payee are in the region.

For electronic payment transactions, a common form of SCA is the application of 3D-Secure. Although it was highly recommended it wasn't always required, merchants had the option to route a transaction through 3DS which would enable a shift in liability where a loss may occur. However, in future, the application of SCA will no longer be optional. There are actions that can be taken today to ensure that you are ready for when the SCA mandate is enforced.

We recommend that you consider how these SCA changes could impact your transaction flow and your customer journey. Depending on the design of the payment experience and operating model, SCA may have different implications for your business.

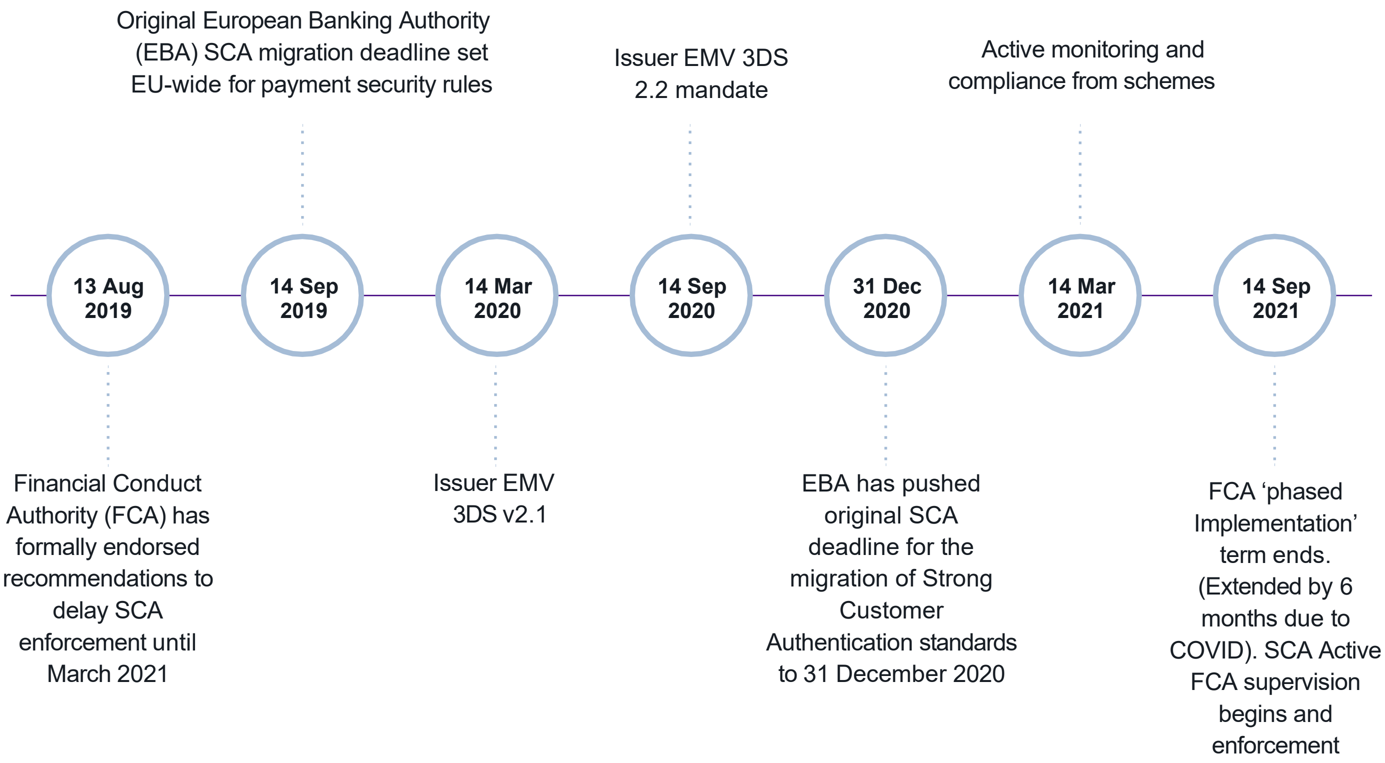
Customer authentication is considered to be strong if it is based on the use of two or more of the following elements

Something they KNOW
(Password, pin, secret

Something they OWN
(Phone, wearable, hardware

Something they ARE
(Fingerprint ID, Facial ID Voice

SCA Roadmap



13 Aug 2019
Financial Conduct Authority (FCA) has formally endorsed recommendations to delay SCA enforcement until March 2021

14 Sep 2019
Original European Banking Authority (EBA) SCA migration deadline set EU-wide for payment security rules

14 Mar 2020
Issuer EMV 3DS v2.1

14 Sep 2020
Issuer EMV 3DS 2.2 mandate

31 Dec 2020
EBA has pushed original SCA deadline for the migration of Strong Customer Authentication standards to 31 December 2020

14 Mar 2021
Active monitoring and compliance from schemes

14 Sep 2021
FCA 'phased Implementation' term ends. (Extended by 6 months due to COVID). SCA Active FCA supervision begins and enforcement

What is 3D-Secure?

3D-Secure (3DS1)

3DS1 was introduced in 1999, to reduce fraud for online transactions. It was designed to add an additional layer of security that would reduce the chance of a chargeback or dispute and allow a card issuer to prove that the shopper attempting a purchase was the legitimate cardholder for the debit/credit card being used.

When 3DS1 was first introduced, smart technology was in its infancy. Whilst 3DS1 has been a powerful and widely adopted anti-fraud solution, shoppers are still put off by browser-based challenges which require them to remember a number of characters from their static password. This leads to a lot of cart abandonment and loss of transactions and a drop in revenue due to the friction this may cause.

EMV 3DS (3DS2)

Modern problems require modern solutions and this is why the new 3DS2 protocol was introduced. 3DS2 is designed to improve upon its predecessor (3DS1) by delivering a much smoother and well integrated experience.

3DS2 adds support for mobile applications without the need to redirect a cardholder to an external website or browser to complete their authentication speeding up the transaction checkout process by almost 80% in a frictionless authentication flow. The quality and accuracy of the data provided in 3DS2 can directly influence the likelihood of a successful authentication in a frictionless manner.

Previous analysis carried out by the card schemes show that the increase in data collection, such as consumer's device information, improves fraud detection by up to 3 times.

3DS Version Fallback

A request for 3D Secure authentication can take 2 routes depending on the version support offered by the entities involved.

With 3DS1, shoppers are usually re-directed to a card issuer's site to provide additional authentication data such as password or a SMS verification code.

With the new 3DS2 version, the card issuer initiates the authentication within the merchant's website or mobile

Benefits of SCA & 3DS

1	Better Intelligence	3DS2 will collect up to 10X more data such as; device data and card holder's shopping history	Issuers can make better risk-based authentication decisions
2	Speed-Up Authentication	The larger contextual data exchange, allows for a more accurate verification of a cardholder's identity	More frictionless authentications Fewer credentials requests
3	Decreased Fraud Level	Reduces fraud, and seeks further cardholder authentication for higher risk transactions	Reduces merchant exposure to chargebacks or disputes
4	Extended integration Support	Supports transactions and check-out integrations on a wider range of platforms and consumer devices	Mobile banking applications integration and biometric and One Time Passwords (OTP)
5	Increases Transaction Approval Rate	Reduced levels of cart abandonment and improved rates of transaction success	Boost in revenue & greater consumer satisfaction

Transaction Success

Transaction success is just as important for Cashflows as it is for its customers.

Increase in Declines
Failure to adhere to PSD2 regulatory changes and to apply SCA to all qualifying electronic payments can lead to an increase in declined transactions and a decrease in revenue.

Exemption Success
It's important to remember that an exemption does not guarantee an authorisation. However, the correct use of an exemption provides a transaction with a much better chance of success. Even when an exemption is requested, the card issuer makes the ultimate approval decision.

Soft Decline
The number of 'Soft Declines' is expected to rise. A 'Soft Decline' can happen when a card issuer does not approve a transaction request with a specific exemption reason code. In this situation, the merchant must set up that transaction using 3D Secure and re- submit it.

Out-of-Scope Transactions

Transactions in the MOTO channel

- Mail orders and Telephone orders (MOTO) do not require SCA (booking over the phone or mail).
- Stronger monitoring will be needed to ensure this channel is safeguarded against elevated fraud risk.

Merchant-initiated transactions

- Payments taken under the continuous payment authority are all initiated by the merchant.
- The initial set up of the recurring payment will still require authentication but all following transactions will be exempt.
- Direct debits, incremental or delayed charges such as late and additional charges on a hotel bill after one has checked out for example.

One-leg-out (OLO) transactions

- The card is issued outside of the EU.
- The customer's bank is outside of the EU (for credit transfers).
- All connections in are to a geographically local server.

Unattended Terminals

The following transactions are out of the scope of the SCA requirement:

- Payments for transport fares.
- Unmanned Road Tolls where a card may be used in an automatic payment machine.
- Car parking fees at an unattended terminal.

Transactions that meet the above criteria are out of scope of SCA requirements

SCA Exemptions

Only a limited defined set of transactions are exempt from the EU's PSD2 requirement for SCA. These are described below.

Although exemptions are a great way to create a frictionless experience for a consumer, it is important to remember that Cashflows strongly suggests that SCA is applied to as many transactions as possible as this will ensure the best possible approval rate. As a result, initially whilst SCA is being rolled out, only recurring or merchant initiated payments where the cardholder is "off session" will qualify for an exemption, however Cashflows will continually monitor our offering and update these in order to bring merchants the most appropriate, effective and safe way of processing transactions.

Low value
Card transactions below €30 are considered low value and are generally exempt from authentication. However, if the customer initiates more than five consecutive low value payments for the same cardholder or if the total payments value exceed €100, SCA will be requested by the issuer.

Merchant initiated transactions (MIT)
MITs defined under this category are performed to fulfil a business practice as a follow-up to an original cardholder merchant interaction that could not be completed with one single transaction such as: additional charges on a hotel bill, where the customer has chosen to use an express checkout service for example.

Trusted merchant (Whitelisting)
Customers will have the option to 'whitelist' a merchant they trust. They can request to have the trusted merchant added to their record with the issuers after the first authentication is completed. Subsequent transactions with the whitelisted merchants are likely to be exempt from future authentication.

Secure corporate payments
When the transaction is initiated by a legal person (e.g. a business) rather than a consumer, and it is processed through a secured dedicated payment protocol, there will not be a requirement for separate authentication, provided alternative controls are sufficiently secure. This should include 'secure virtual payments', such as virtual cards or B2B cards.

Low-risk Transaction (TRA)
This exemption has by far the largest scope on any transactions below €500. Merchants would have to request this exemption from their acquirer. However, the total fraud exposure across all of their customers should remain below the specified fraud rate exemption limits.

Recurring payments
A series of payments of the same value to the same merchant (such as subscriptions and membership fees) are exempt after the initial set up. The initial set up of the recurring payment will still require authentication, but all subsequent transactions will be exempt.

How will you be affected?

The requirement for Strong Customer Authentication (SCA) under PSD2 means that authentication of payers is no longer about opting-in. For in-scope transactions, SCA must be carried out. This means card transactions must be authenticated via 3D Secure (or equivalent for other non-Visa and Mastercard brands).

The Cardholder's Bank is ultimately responsible for providing the means of SCA and ensuring SCA is carried out. But the efficient execution of SCA, also requires the involvement of Payment Service Providers (PSP) and Acquirers, in the case of card payments.

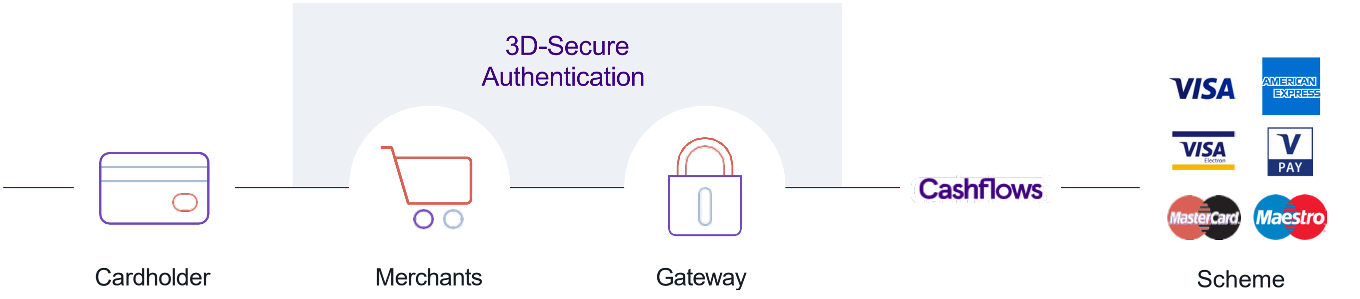


Figure1: The application of strong customer authentication is required in the initiation and processing of electronic payments usually handled by a Payment's Gateway or Third Party Service provider.

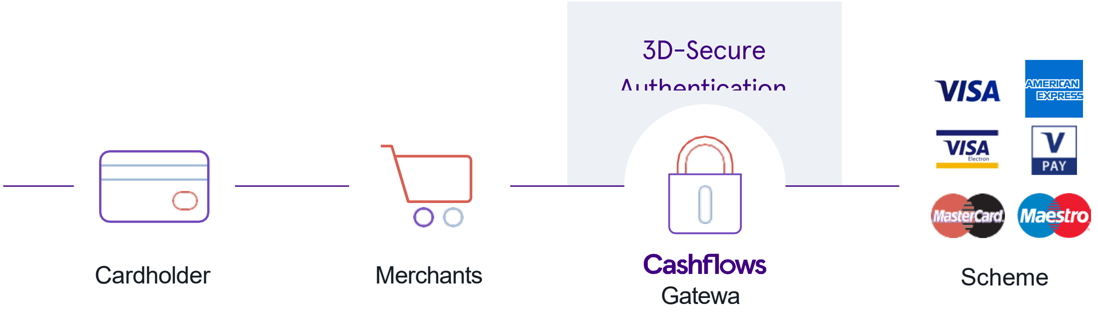


Figure2: In the above figure, Cashflows Gateway will handled the authentication of your cardholders.

There are some things merchants can do now to prepare for SCA by getting 3DS 2-ready. These steps include:

- Ensuring all required fields are being captured in checkout flow
- Prioritizing your development resources to upgrade to the latest protocol of the 3D Secure authentication (3DS 2); For those who outsource their authentication to a third-party service provider then you are responsible for ensuring the adopted solution is SCA compliant.

Cashflows Integration Methods

Hosted Payment Page
Merchants using our legacy ‘Hosted Payment Page’, will be contacted in order to discuss the migration path to Cashflows new SCA 3DS v2 compliant solution.

Transactional APIs
We have made some changes and extended to our transactional APIs to comply with PSD2 requirements as well as enabling support for new EMV 3DS protocol fields.

Important
Merchants and Gateways who use one of our transactional APIs are advised to review the technical guides and documentation found in the support section of our website to establish the impact of these changes on future transactions.

Are you ready?

Our merchant and gateway customers who are directly integrated into our transactional APIs, may need to liaise with their 3DS service provider(s), and prioritise their development resources to upgrade to the latest update of the EMV 3DS protocol.

Merchants will need to amend or change their privacy notice and/or terms and conditions to comply with the GDPR requirements.

Cashflows GDPR guides have been updated to reflect the latest requirements.

Card Issuers are likely to begin declining transactions which have not adhered to the SCA mandate from the 1st January 2021 for EU transactions and 14th September 2021 for transactions within the UK

Are you ready to support the new regulatory requirements?

What’s the future holding?

Cashflows technology stack is modern and resilient, our API driven rich payments functionality is already a cloud based, highly scalable platform and it’s about to get better.

Cashflows will soon be offering ‘top of the range’ gateway services alongside its already successful acquiring services.

Purposely built from the ground up, our gateway will combine many features that will allow our clients to overcome industry problems of today.

It will not only come equipped with a brand new updated and re-designed hosted payment page, but it will also have its own Merchant Plug-in (MPI) solution that incorporates into your website or shopping basket and it will facilitate and drive 3D-Secure authentication of your customers so you don’t have to.

Watch this space…

Cashflows

+44 (0)330 128 9855
sca@Cashflows.com
Cashflows.com

Cambridge
CPC1
Capital Park
Cambridge
CB21 5XE

London
20 Farringdon St
London
EC4A 4AB

The Netherlands
Noorderhof 24
5804 BV Venray