ECOMMERCE PSD2 SCA FAQs

What is Payment Services Directive 2 Strong Customer Authentication (PSD 2 SCA)?

PSD2 was introduced in 2015 as European Union (EU) Directive 2015/2366 throughout the European Economic Area (EEA). The directive was required to be implemented into local law within each country of the EU by 13th January 2018. SCA is a requirement within PSD2 which stipulates that electronic payments are performed with multi-factor authentication, to increase security and reduce fraud. SCA will be fully enforced on 14th March 2022 in the UK.

What authentication requirements does SCA introduce?

Subject to specified exemptions, SCA is mandated for all electronic payment transactions and requires authentication by two or more independent factors. The factors are:

- Knowledge (something only the user knows, i.e. a password)
- Possession (something only the user possesses, i.e. a token or mobile phone)
- Inherence (something that biometrically identifies the user, for example fingerprint recognition or facial scanning)

Who is responsible for the application of SCA?

Payment Service Providers (PSPs) are responsible for the application of SCA. PSPs are defined as regulated Bank Issuers and Acquirers. PSPs must ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors:

- lists of compromised or stolen authentication elements
- the amount of each payment transaction
- known fraud scenarios in the provision of payment services
- signs of malware infection in any sessions of the authentication procedure

Which Clover services will require updates to support SCA?

Clover offers 3 electronic payment services that are affected by PSD2 SCA, namely:

I. Gateway

II. Acquiring

III. Processing

We are working closely with national regulators and payment schemes to ensure that our services are PSD2 SCA compliant and that they can support all out of scope and exempt electronic payment categories to ensure the best possible authorisation outcomes for our merchants.

In what countries does SCA apply?

The list of countries in scope for SCA by virtue of being in the EEA are as follows:

- Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, and Sweden. While the UK is no longer in the EEA, SCA will still be enforced.

What is SCA Dynamic Linking?

For electronic payments under SCA, each authentication event must be linked to a specific amount and payee (dynamic linking). This requirement, effectively binding authentication to the payee and the amount, aims at ensuring that a valid authentication code is only used once and for the specific electronic payment for which the authentication is requested. The objective is to reduce “man in the middle” attacks.

To which electronic payment categories does SCA apply?

SCA must be applied to the following electronic payment categories:

I. Making a remote card payment transaction through the internet.
II. Online-banking based credit transfers under which the payer uses an online banking portal for authentication.
III. Payments through e-payment providers, with which the consumer has set up an individual account. Accounts can be funded through ‘traditional’ payment methods, for example bank transfers or credit card payments.
IV. Remote m-payments mostly take place through internet/WAP9 or through premium SMS services which are billed to the payer through the Mobile Network Operator (MNO).
V. Proximity payments generally taking place directly at the point of sale.

Are any payment categories out of scope for SCA?

A number of electronic payment categories are out of scope for PSD2 SCA. These categories are outlined in Table 1 below.

Table 1 – Electronic Payment Categories out of scope for PSD2 SCA

#	Electronic Payment Category	Description
1	Direct Debits	A payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the consent given by the payer to the payee, to the payee's payment service provider or to the payer's own PSP.
2	Payee/Merchant Initiated Transactions	A transaction, or series of transactions (variable subscriptions), of a fixed or variable amount and fixed or variable interval governed by an agreement between the payer and payee/merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the payer. **Note:** Payee's will be required to send the transactions ID of the original Customer Initiated Transaction (CIT) in order to qualify their MIT transactions as out of scope for SCA.
3	Mail Order Telephone Order (MOTO)	Payments transacted over the phone are not considered to be electronic payments and are therefore deemed out of scope for SCA.
4	Anonymous payment instrument transactions	Payment instruments that can only be identified by the Issuing Bank such as anonymous prepaid cards.
5	Inter-regional payments	Electronic payments where the payment instrument is issued by an Issuer outside the EEA or where the country where the Acquirer is domiciled is outside the EEA. For multi-national merchants who process payments around the world, including in the EEA, this is particularly relevant.

Will SCA be required for all other eCommerce transactions?

SCA will be required for all cardholder-initiated eCommerce transactions that are not out of scope as detailed above, unless an SCA exemption is available and relied upon. After 14th March 2022 transactions that have not been authenticated using multi-factor authentication (like 3D Secure 2.0) and do not qualify for an SCA exemption, will be declined/at risk of fraud

Is SCA required for alternative payment methods?

Alternative payments are defined as non-card electronic payments under PSD2, and in most circumstances they will need to meet SCA requirements. Credit transfers, also known as real time bank transfers, offered by banks and schemes like iDeal, Giropay and Sofort, require the payers to pay via their bank account through their online banking access. These credit transfers have already implemented SCA so there will not be any changes to the payer experience when using them. Invoice solutions such as Klarna also already meet SCA requirements. Transfers between a user's own accounts at the same institution do not require SCA (see item 7 in Table 2 below).

To which payment categories can SCA exemptions be applied?

A number of electronic payment categories are eligible for exemptions under PSD2 SCA.

These categories are outlined in Table 2 below.

Table 2 – Electronic Payment Categories eligible for exemption under PSD2 SCA

#	Electronic Payment Category	Description
1	Low value	Electronic payments under €30 on a payment instrument. This applies when the cumulative amount of previous electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed €100 or the number of previous electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed five consecutive individual electronic payment transactions.
2	Subscription or recurring transactions with a fixed amount	Payer initiated recurring payments for the same amount, to the same payee. SCA will be required for the payer's first payment - subsequent payments are exempt.
3	Trusted beneficiaries (Whitelisted payees/merchants)	Payers can assign payees to a whitelist of trusted beneficiaries maintained by their bank. Whitelisted payees will be exempt from SCA.
4	Secure corporate payments	Electronic payments made through dedicated corporate processes initiated by businesses and not available for consumers. These include payments made through central travel accounts, lodged cards, virtual cards, and secure corporate cards.
5	Contactless payments	The value of the electronic payment via a mobile device at point of sale must not exceed €50; and › The cumulative limit of consecutive contactless transactions without application of SCA must not exceed €150 or › The number of consecutive contactless transactions since the last application of SCA must not exceed five
6	Unattended transport and parking terminals	Electronic payments via unattended terminals for transport fares and parking fees.
7	Credit Transfers between the same natural or legal person	Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a credit transfer in circumstances where the payer and the payee are the same natural or legal person and both payment accounts are held by the same account servicing payment service provider.

<table>
<tr><th>#</th><th>Electronic Payment Category</th><th>Description</th></tr>
<tr><td>8</td><td>Low-risk transactions/ Transaction Risk Analysis (TRA)</td><td>
<p>For certain lower value transactions, a PSP will be allowed to do a real-time risk analysis to determine whether to apply SCA to a transaction. This is only possible if the PSP's fraud rates do not exceed the following thresholds:</p>
<table>
<tr><th>PSP Fraud Rate Threshold</th><th>Electronic Payment Exemption bands</th></tr>
<tr><td>13 bps/0.13%</td><td>Up to £85</td></tr>
<tr><td>6 bps/0.06%</td><td>£85- £220</td></tr>
<tr><td>1 bps/0.01%</td><td>£220 - £440</td></tr>
</table>
<p><b>Note:</b> PSD2 requires the fraud rate to be assessed at the PSP level, as it cannot be assessed on an individual basis for a specific merchant.</p>
<p>If an electronic payment under TRA is in a non-Euro currency, a currency conversion will need to be applied to determine whether or not it qualifies. The rate to use for this conversion has not yet been determined.</p>
</td></tr>
</table>

What happens to transactions that are not SCA authenticated and do not qualify for an exemption?

Transactions that don't meet these new authentication requirements and do not qualify for any exemption may be declined after the regulation comes into effect on 14th March 2022. 3D Secure 2.0 will be the primary authentication method used to meet SCA requirements for all eCommerce transactions.

What is 3D Secure?

3D Secure is the global specification for card payment security developed by EMVCo. EMVCo is collectively owned by American Express®, Diners Club International®, Discover Global Network®, JCB®, Mastercard®, UnionPay® and Visa®.

What is 3D Secure 1.0?

3D Secure 1.0 is an authentication process introduced to reduce online fraud and enable the cardholder to make safe and secure online payments. 3D Secure 1.0 has been criticized for providing a poor user experience for cardholders, especially when they're using a mobile device, which has led to an increase in checkout abandonment.

What is 3D Secure 2.0?

3D Secure 2.0, also known as EMV® 3-D Secure, is the updated version of 3D Secure 1.0, which has been on the market for some time within branded products like Verified by Visa®, MasterCard SecureCode®, and SafeKey by American Express®. 3D Secure 2.0 is a new version of authentication, designed to be frictionless, faster, and safer, removing the old redirect of 3D Secure 1.0 and replacing it with a dynamic bridge between the issuing banks and merchants that analyses customer shopping patterns. For example, past purchases, ship-to locations, and purchase amount which will allow cardholders to authenticate transactions in innovative new ways e.g. with their finger print or through facial recognition. 3D Secure 2.0 will be the primary authentication method used to meet SCA requirements for eCommerce transactions.

How does 3D Secure 2.0 differ from 3D Secure 1.0?

The key differences between 3D Secure 1.0 and 3D Secure 2.0 are as follows:

- Improved messaging with supplementary information for better decisions on authentication
- Non-payment user authentication
- Non-standard extensions to meet specific regulations and requirements, including proprietary out-of-band authentication solutions, used by Card Issuers
- Better performance for end-to-end message processing
- Improved datasets for risk-based authentication
- Prevention of unauthenticated payment, even if a cardholder's card number is stolen or cloned
- Enhances functionality that enables merchants to integrate the authentication process into their checkout experiences, for both app and browser-based implementations
- Enables merchant-initiated account verification
- Supports specific app-based purchases on mobile and other consumer devices

How will this impact your business?

If you do not implement 3D Secure 2.0 and/or avail of appropriate exemptions you may experience a high rate of declined card transactions from 14th March 2022 onwards. In fact, since 1st June 2021 UK issuing banks have gradually started to decline transactions that do not comply with SCA rules. This will increase significantly as the 14th March 2022 full compliance date approaches

Does Clover support 3D Secure 1.0?

Clover supports 3D Secure 1.0 on the Clover Gateway and on our payment processing platforms. Merchants can use our integrated Merchant Plug-in through our Hosted Payment Pages or via our Web

Service API. Merchants can also choose to use a 3rd party MPI and simply authorise through Clover Gateway and we can also facilitate that.

Does Clover support 3D Secure 2.0?

Clover supports 3D Secure 2.0 on the Clover Gateway and on our payment processing platforms. Merchants can use our integrated Merchant Plug-in through our Hosted Payment Pages or via our Web Service API. The merchant can also choose to use a 3rd party MPI and simply authorise through Clover Gateway. We want to help our merchants and their payers have the most secure and frictionless experience possible under PSD2 SCA and correctly handling out of scope electronic payment categories is key to achieving that.

Beyond ensuring compliance with PSD2 SCA requirements, what are the additional benefits of 3D Secure 2.0 for merchants?

3D Secure 2.0 requires more data to validate a cardholder's identity, compared to its predecessor 3D Secure 1.0. This means there are more opportunities to limit eCommerce fraud by providing more information to prove the cardholder's identity. This will allow merchants to manage fraud more easily, increase the number of authenticated transactions and provide a better user experience at checkout through multiple payment channels.
As a merchant, the benefits also include:

- Optimised checkout incl. mobile, in-app, web
- Reduced checkout abandonment
- Control over the transaction risk they assume
- Higher conversion rates due to frictionless checkout
- Reduced fraud
- Reduced interchange fees
- Liability shift for all authenticated transactions
- Compliance with the PSD2 SCA requirement

As a Clover Gateway merchant what do I do next?

Clover Gateway merchants can access our 3D Secure 2.0 solution where they can flag out of scope and exempt electronic payment categories.

The Clover Gateway integration documentation for 3D Secure 2.0 is available here: https://docs.firstdata.com/org/gateway/node/456. We advise you to access this and make the small adjustments required to your integration in order to implement 3D Secure 2.0 immediately. If you do not, you may experience a high volume of declined transactions.

How can Clover help if you use a Third Party Gateway?

If you do not use the Clover Gateway it is important that you contact your gateway provider (or PSP) as soon as possible to ensure that you ready your business for the changes that are required to continue to successfully transact from 14th March 2022 onwards. Alternatively merchants can contact us on 0345 606 5055 to discuss using the 3D Secure 2.0 compliant