First Data.

ECOMMERCE PSD 2 SCA FAQs

What is Payment Services Directive 2, Strong Customer Authentication (PSD2 SCA)?

PSD2 is a European Union (EU) Directive which was launched in 2015.

SCA is a requirement of PSD2, designed to increase security and reduce fraud by ensuring electronic payments are performed with multi-factor authentication.

When does it come into effect?

Subject to specified exemptions, SCA is currently due to become a mandatory requirement for all electronic payment transactions on 14th September 2019.

What authentication requirements does SCA introduce?

SCA 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 transaction monitoring mechanisms are in place.

In what countries does SCA apply?

All countries within the EEA are in scope for SCA.

196955-0416

First Data.

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 online wallet providers which can be funded through 'traditional' payment methods, for example bank transfers or credit card payments.
IV. Remote mobile payments mostly take place through the internet or your 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 card 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	Merchant Initiated Transactions (MIT)	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) from September 14th in order to qualify their MIT transactions as out of scope for SCA.
2	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.
3	Anonymous payment card/device transactions	Payment card/device that can only be identified by the Issuing Bank such as anonymous prepaid cards.

#	Electronic Payment Category	Description
4	Inter-regional payments	Electronic payments where the payment card/device 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 September 2019 transactions that have not been authenticated using multi-factor authentication (like EMV 3-D Secure) and do not qualify for an SCA exemption, will be declined/at risk of fraud

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 or equivalent GBP unless the Issuer requires SCA.
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.

#	Electronic Payment Category	Description
5	Contactless payments	The value of the electronic payment via a mobile device at point of sale must not exceed €50 or equivalent GBP unless the Issuer requires SCA.
6	Unattended transport and parking terminals	Electronic payments via unattended terminals for transport fares and parking fees.

Full details can be found on our website www.firstdata.com/3DSecure2.0FAQ or through your eCommerce provider.

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

Transactions that do not meet these new authentication requirements and do not qualify for any exemption may be declined after the regulation comes into effect on 14th September 2019. 3D Secure 2.0 will be the primary authentication method used to meet SCA requirements for all eCommerce transactions.

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.

Will 3D Secure 1.0 still work after 14th September 2019?

We expect that from 14th September 2019, some EEA Issuing Banks may only be able to support 3D Secure 1.0. Therefore we recommend that merchants/payees support 3D Secure 1.0 until the card schemes' end support for 3D Secure 1.0, which will be somewhere between 2020 and 2021.

What is EMV 3-D Secure? (also known as 3-D Secure 2.0)

EMV 3-D Secure, also known as 3-D Secure 2.0, is a new version of authentication within branded products like Verified by Visa®, MasterCard SecureCode® and is 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. EMV 3-D Secure will be the primary authentication method used to meet SCA requirements for eCommerce transactions

How does EMV 3-D Secure **differ from** 3-D Secure 1.0**?**

The key differences between 3-D Secure 1.0 and EMV 3-D Secure 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

Does First Data support 3D Secure 1.0 and EMV 3-D Secure?

First Data payment processing platforms support both 3D Secure 1.0 and will support EMV 3-D Secure before the implementation date of 14th September 2019.

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

EMV 3-D Secure 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 First Data Gateway merchant what do I do next?

The First Data Gateway integration documentation for EMV 3-D Secure is available here: https://docs.firstdata.com/org/gateway/node/456. You are required to access this and make the small adjustments needed to your integration in order to implement EMV 3-D Secure before 14th September. If you do not, you may experience a high volume of declined

transactions from this date onwards. Questions with regards to your integration to the First Data Gateway should be directed to our helpdesk team 0345 606 5055.

How can First Data help if you use a Third Party Gateway?

If you do not use the First Data Gateway it is important that you contact your gateway provider (or PSP) as soon as possible to ensure that your business is ready for the changes that are required to continue to successfully transact from 14th September 2019 onwards. Alternatively merchants can contact us on 0345 606 5055 to discuss using the 3D Secure 2.0 compliant First Data Gateway.