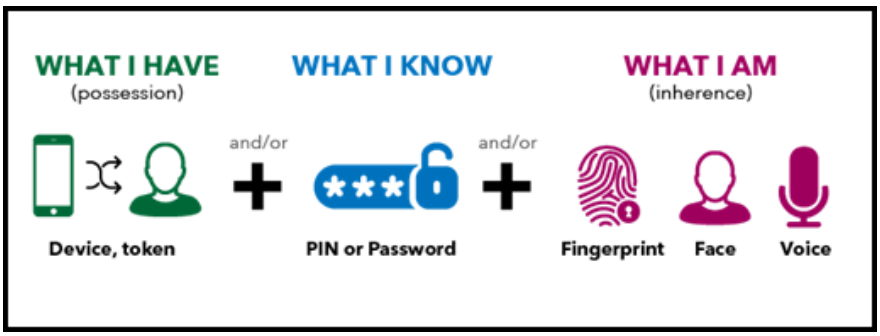
LLOYDS BANK

Strong Customer Authentication Frequently Asked Questions

What is Strong Customer Authentication?

Strong Customer Authentication (SCA) is a European regulatory programme which focuses on increasing the security of online payments. By 14 September 2021, all banks will be asking their cardholders to authenticate themselves using two methods of authentication. Your customers will need to authenticate using two of the three categories to access their accounts, make payments or complete other high-risk transactions such as changing their telephone number. This can be something they know (e.g. a password), something they have (e.g. a mobile phone) or something unique to them (e.g. a finger print).



As a result of this, technical changes may be required to your website to comply with these regulations. We have contacted your payment service providers to notify them of the requirements, and we would advise you to speak to them about this change. As well as a card scheme mandate, there is a legal obligation to deliver strong customer authentication.

What countries does this regulation apply to?

This regulation applies to all EEA countries, which are:

Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, UK, Iceland, Liechtenstein and Norway.

What happens if the cardholder isn't in one of the countries listed above?

If the card is issued outside the EEA you may not be required to attempt Strong Customer Authentication – although, from a fraud and liability perspective merchants should risk assess every transaction and consider using 3D Secure to request authentication if a transaction looks to be high risk.

How will it impact my business?

Unless the transaction meets one of the exemption requirements, customers will now need to go through a 2 factor authentication process. This will be a significant change for businesses that do not use a service such as 3D Secure and those that do may need to submit more transactions for authentication.

Are there times when I don't need to attempt Strong Customer Authentication?

Where an exemption may be applicable, it is down to the each Issuer and Acquirer to decide whether or not it can be applied. Cardnet is currently working through its strategy for the application of exemptions.

In some circumstances, there may be an exemption that can be applied to specific online payments. These are:

- Transactions of low value – 2 factor authentication is not required for remote electronic transactions when the transaction amount does not exceed £30, or does not exceed 5 transactions, or £90 cumulative spend, since they last verified their identity. This exemption can be applied by either the issuer or acquirer.
- Transaction risk analysis – 2 factor authentication may not be required for transactions that meet certain fraud rate thresholds. These will only be considered on an exceptional basis and subject to certain additional criteria.

This exemption can be applied by either the issuer or acquirer.

Whitelisting – two-factor authentication is not required for transactions where the merchant has been listed by the cardholder as a trusted beneficiary. This may be a merchant that the cardholder often uses. This exemption can only be applied by the issuer. Two-factor authentications is required when the cardholder adds or amends a trusted beneficiary

Mail order and telephone order (MOTO) and merchant initiated transactions are out of scope and do not require two-factor authentication

A merchant initiated transaction is a transaction that is taken at an agreed date, with the cardholders consent and it is initiated by the merchant. For example, a recurring payment for a mobile phone bill or a monthly subscription. The cardholder has given consent to take a future payment, which often occurs around a similar date.

Contactless – there are some changes to contactless payments as issuers are required to limit the total amount or number of transactions a customer can make before they are required to use Chip and PIN. You should ensure your terminals are updated to handle new "soft-decline" responses from issuers.

Can I apply for these exemptions?

Cardnet can advise you on what exemptions may be applicable for your business.

What should I do now?

Merchants should speak to their acquirers, gateways and trade associations to understand the steps they need to take in order to prepare and meet the agreed timeline, including understanding:

- Which version of 3D Secure you will use
- Which exemptions may apply and how to use these
- Dates for testing
- Date for go-live.

You should understand your plans as soon as possible due to the amount of change that might be required.

Cardnet can work with you to obtain a clear plan to accelerate towards operational readiness and align with Scheme mandates.

What will happen to my transactions after 14 September 2021 if I do not make any changes?

Issuers will have to decline all non-SCA-compliant transactions after this date, and therefore all merchants, gateways and acquirers need to be ready to support SCA to avoid consumers having declined ecommerce transactions from this date. Merchants who take payments from customers from other EEA countries may need to support SCA by 31 December 2020.

Further guidance can be found via the UK Finance website which includes detailed implementation plans, these can be accessed via the below links.

- Overview of Strong Customer Authentication rollout
- Ensuring UK SCA compliance and minimising customer impact
- Strong Customer Authentication: Communication on improving outcomes from 3DSecure – Data Consistency
- UKFI Guidance on Strong Customer Authentication under PSD2

Does my payment service provider know about the changes required?

Yes, we have contacted all Payment Service Providers who send your transactions into us for processing to advise them of the changes. We would encourage you to speak to them directly about any technical changes you may be required to make in order to comply with the requirements.

What does SCA mean in terms of chargeback liability?

- 3D Secure ecommerce transactions – Issuer is liable
- Non-secure e-commerce transactions with the merchant exemption flag i.e. no 3D Secure sent directly for authorisation – Merchant is liable
- Non-secure e-commerce transactions with the transaction risk analysis exemption flag i.e. no 3D Secure, sent directly for authorisation – Merchant is liable
- Trusted beneficiaries – Issuer liable
- Merchant Initiated transactions – Merchant is liable

Transaction Type	Merchant Liable for Fraud?	Issuer Liable for Fraud?
3D Secure Transaction	No	Yes
Non-Secure (with exemption flag)	Yes	No
Non-Secure (risk analysis exemption flag)	Yes	No
Trusted Beneficiaries	No	Yes
Merchant Initiated Transactions	Yes	No

I take payments from outside the UK – am I still affected?

Regulatory enforcement dates, and the conditions for any enforcement delay, may differ between markets as determined by national regulators. For example, SCA enforcement for e-commerce will begin in the UK on 14 September 2021, however SCA will be enforced by national regulators in much of Europe from 1 January 2021. From the regulatory enforcement date in any given market, all transactions originating online must be authenticated when they are in scope of the SCA regulation unless an exemption applies.

Cardnet therefore recommends that any Merchant accepting payments from other EEA countries should plan to be ready to comply with SCA regulation prior to January 2021 so as not to see declines in these types of payments. In readiness for the European Banking Authority deadline for SCA enforcement in e-commerce (31 December 2020) some Merchants may begin to see a proportion of payments soft decline from as early as October 2020.

What are the SCA requirements for Travel and Hospitality Suppliers and Merchants and those who operate split-shipment?

Travel and hospitality merchants should be ready for SCA by 31 December 2020, even if not all parties in their booking chain are ready. This means that in-scope payments processed without the cardholder available to initiate or authenticate the transaction (i.e. partial or full upfront deposits / payments during an online booking, balance payments prior to check-in or cancellation fees) can no longer be submitted via manual key entry into the point-of-sale system without proof of authentication.

Instead, the following requirements will apply:

- The cardholder needs to be authenticated at the time of booking.
- The authorisation request for such payments must be sent with either a proof of authentication (i.e. the 3D Secure data) or a reference to it (i.e. the transaction ID of the authorised transaction where the agreement for the merchant to process a merchant-initiated transaction [MIT] was set up).

Merchants who split ship goods and travel and hospitality merchants who split the bookings to multiple parties (i.e an agent model), may in some instances use the Cardholder Authentication Verification Value (CAVV) up to five times within a six month period, up until 1 September 2022.

Further information on the options for travel and hospitality suppliers to ensure authentication can be found on the link below:

http://click.broadcasts.visa.com/xfm/?41054/0/8344f6a350e4328d912b46ebf76446ea/lonew

I still have further questions – who do I contact?

We have set up a dedicated mailbox for any further questions on Strong Customer Authentication – please contact:

CardnetSCAQueries@lloydsbanking.com