COMMERCIAL BANKING

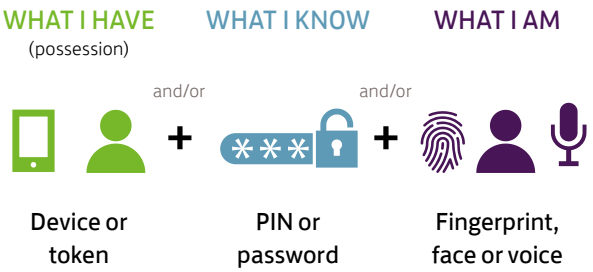
STRONG CUSTOMER AUTHENTICATION

FREQUENTLY ASKED QUESTIONS

What is Strong Customer Authentication?

Strong Customer Authentication (SCA), a new regulation being introduced to make online payments more secure. Your customers will have started to see extra checks when making online payments from June 2021 and will see more of their payments going through these checks over the coming months. From 14 March 2022 all online and recurring payments will be checked. This date has changed from 14 September 2021 to give businesses more time to get ready for SCA. By 14 March 2022, all UK Card Issuers will be asking their cardholders to authenticate themselves using two methods of authentication for some online payments. Your customers will start to see more requests to authenticate using two of the three categories when they make payments via Websites, Apps and payment URLs/links or set up recurring payments.

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 and authentication tools 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.

If you currently use us as your acquirer and payment gateway or services provider, there's nothing for you to do. Your online payments will comply with SCA.

What countries does this regulation apply to?

This regulation is effective from 14 March 2022 in the UK. For the remainder of the countries in the European Economic Area (EEA), listed below, this regulation came into effect on 31 December 2020. Although each country has chosen a differing timeline to enforce the regulation depending on its market readiness.

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, 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 (3DS) to request authentication if a transaction looks to be high risk.

LLOYDS BANK

How will it impact my business?

From 1 June 2021 if you use other payment service providers unless the transaction is deemed out of scope of SCA regulation or one of the available exemptions is applied, your customers transactions may need to be authenticated via 3D secure , failure to do so may result in declined transactions. This will be a significant change for businesses that do not use a service such as EMV 3DS. To help you decide which authentication tools your business will benefit from we have provided more detail in our SCA EMV 3DS Brochure.

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

Where an exemption may be applicable, it is down to each Card Issuer and Acquirer to decide whether or not it can be applied.

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

- **Transactions of low value** – two-factor authentication may not be required for remote electronic transactions when the transaction amount does not exceed £25, or does not exceed five transactions, or £85 cumulative spend, since they last verified their identity. This exemption can be applied by either the Card Issuer or Merchant with agreement from the Acquirer.
- **Transaction risk analysis** – two-factor authentication may not be required for transactions that meet certain fraud rate thresholds. This exemption can be applied by the Merchant with agreement from the Acquirer and are subject to certain additional criteria. Please contact us to discuss options available to you.

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 authentication is required when the cardholder adds or amends a trusted beneficiary.

Mail order and telephone order (MOTO) and Merchant Initiated Transactions (MITs) are out of scope of SCA regulation and do not require authentication however to remain SCA compliant and ensure they do not get declined they must be flagged correctly by Merchants. To ensure correct flagging please speak with your Payment Gateway.

A Merchant initiated transaction (MIT) 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.

However please note further information on reoccurring MITs can be found later in this document.

Can I apply for these exemptions?

There are some important factors to consider prior to applying to Cardnet for any exemptions. Firstly, it is important to understand that liability for these transactions will move from the Card Issuer to the Merchant. Secondly Merchants may also require a comprehensive Fraud Tool to ensure effective monitoring of transactions which are flagged as exempt. For more information on our Fraud Tool or how you can apply for an exemption please contact us directly to discuss your requirements.

What will happen to my transactions after 14th March 2022 if I do not make any changes?

Merchants who take payments from customers from other EEA countries may have been required to support SCA since 31 December 2020. To prepare UK Consumers in advance of the deadline a percentage of transactions will be soft declined, meaning cardholders will be prompted to apply two factor authentication to complete a transaction. In the UK this will be from 1 June 2021. By these dates you should be ready to process transactions in line with SCA regulations: either request authentication via a version of 3DS or identify a transaction as exempt/out of scope in the authorisation request. From the enforcement date of 14 March 2022 all Issuers will have to decline all non-SCA-compliant transactions, All Merchants, Payment Gateways and Acquirers need to be ready to support SCA to avoid consumers having declined ecommerce transactions.

Does my Payment Service Provider know about the changes required?

Yes, we have contacted all Payment Service Providers and Payment Gateways 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 to comply with the requirements.

Clients who store card details and submit recurring payments (MITs)

Merchant Initiated Transactions (MITs) are exempt from SCA requirements due to the cardholder not being present to authenticate. However, from the SCA enforcement date, any new MITs will be required to have an associated EMV 3DS2 cryptogram, this will provide evidence to the Card Issuer that the first transaction has completed card holder two factor authentication.

To ensure cardholders are not inconvenienced the term and process of 'grandfathering' has been introduced by the Card Schemes. To prove a card was previously stored and submitted prior to the introduction of SCA regulation the card schemes require the completion of certain fields to alert the Issuer to the fact that the card is a MIT and does not need to be authenticated. These fields vary for each Card Scheme as set out below. We recommend discussing your requirements with your Payment Gateway provider, who will be able to advise you on the below.

VISA
3DS Requestor Prior Transaction Reference = DS Transaction ID of the initial Recurring Payment Agreement authentication. This reference is a must to complete the authentication process successfully. If you do not have the original Transaction ID and are unable to attach a EMV 3DS2 cryptogram please contact us to discuss.

Mastercard
DE 48 SE 63 = Trace ID of the initial Recurring Payment Agreement. This reference is a must to complete the authentication process successfully. The Trace ID includes the Banknet Reference Number (BRN). The BRN will be set to "999999" if the agreement was concluded before 14 March 2022 (UK).

Merchants must therefore make the appropriate changes to their MITs to ensure the transactions are accepted seamlessly from 14 March 2022 (UK), however we recommend testing prior to this date to avoid declines. We recommend discussing your requirements with your Scheme representatives and Payment Service provider.

What does SCA mean in terms of chargeback liability?

Mastercard is revising its standards to decrease incidents of friendly fraud. Friendly fraud is often the result of unrecognisable merchant identifiers in transaction details. Cardholders mistakenly initiate chargebacks because they simply do not recognise the purchase or merchant descriptor. Accordingly, Mastercard is aiming to reduce costs related to chargebacks and disputes.

To enable greater transparency and reduce fraud for the benefit of all participants in the payment ecosystem, Mastercard is requiring merchants to provide business logos for Mastercard use in accordance with the agreed terms and conditions from the Logo Microsite. With digital logos from merchants, Mastercard is able to provide enriched post-transaction data to cardholders to help them identify valid purchases and reduce billing problems. The Logo Microsite is available at https://logo.ethoca.com.

Transaction type	Merchant liable for fraud?	Issuer liable for fraud?
EMV3DSecure Transaction	No	Yes
Non-Secure (with exception flag)	Yes	No
Non-Secure (TRA-risk analysis exception flag)	Yes	No
Trusted Beneficiaries	No	Yes
Mail Order/Telephone (MOTO) or Merchant Initiated Transactions (MIT)	Yes	No

I use 3DS Version 1 am I compliant?

You will see from the table below that different versions of 3 D Secure offer differing liability protection and functionality.

From 16 October 2021 if a card issuer chooses not to support 3DS Version 1, there will also be no Visa stand-in, which means no authentication is performed and you the merchant retains fraud liability if the transaction is accepted. This could mean that where there is a dispute or chargeback as a result of fraud, the liability for that transaction resides with the merchant. Prior to the aforementioned date, where 3DS is performed using 3DSv1 you will continue to benefit from the fraud liability protection.

From 14 October 2022 Mastercard will no longer support 3DS v1.0 transactions for cardholder authentication. Any transaction submitted to the Mastercard 3DS v1 will be rejected. Mastercard will continue to support fraud liability until the 14 October 2022.

Our solutions utilise EMV 3DS (v2.1 & 2.2) which provides vastly more data and promotes frictionless cardholder authentication during checkout when compared to 3DS v1. This EMV 3DS v2 specification also supports various transaction flows not supported on 3DS 1.0 including in-app authentication.

If you use an alternative Payment Services Provider or Gateway Lloyds Bank recommends adopting the most up-to-date version, EMV 3DS Version 2.x as soon as possible.

Version comparison and liability protection

Question / Version:	3DS 1.0	EMV 3DS 2.1	EMV 3DS 2.2
Does it support PSD2 SCA compliance?	Yes	Yes	Yes
Provides merchant fraud liability protection when Issuer or Visa or Mastercard attempts server authentication?	Visa: Yes, until 16th Oct 2021 (VBN AI09869 on VOL, subject to issuer participation) Mastercard: Currently offers liability, withdrawal date 14th Oct 2022	Yes	Yes
Supports exemptions and further programs in the authentication flow?	No	Yes, but does not support Trusted Beneficiary (Whitelisting), Delegated Authentication or Transaction Risk Analysis	Yes - Full support
Supports SCA decline code (soft decline) transaction management	Not fully. Limited as it cannot prompt the issuer to challenge the consumer so can lead to subsequent declines	Yes	Yes
Supports a good user experience (UX)	Limited data exchange means more friction flows. Also see SCA decline code management for further poor UX	Better for UX with additional data to support frictionless authentication	Best available solution for managing steps between payment and authentication flow

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 March 2022, however SCA has been enforced by national regulators in much of Europe since 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 in the EEA for SCA enforcement in e-commerce (31 December 2020).

What are the SCA requirements for travel and hospitality suppliers and merchants and those who operate split-shipment?

Visa and Mastercard recommend that all 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 any payments covered under SCA regulation, which are 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 3DS data) or a reference to it (i.e. the transaction ID of the authorised transaction where the agreement for the merchant to process a 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 can be obtained via your schemes representative.

What should I do now?

Merchants who do not use Lloyds Bank as both their acquirer and payment gateway should speak to their third party payment service providers and Payment Gateways to understand the steps they need to take in order to prepare and meet the SCA enforcement timelines.

You should understand your plans as soon as possible due to the amount of change that might be required. Although the enforcement deadline is 14 March 2022, UK Finance has confirmed that UK Card Issuers will begin soft declining a percentage of non 3DS transactions from 1st June 2021 onwards.

Cardnet can work with you to obtain a clear plan to accelerate towards operational readiness and align with Card Scheme mandates. Below is a helpful checklist.

Payment Gateway

- Test the application of MIT flags.
- Check that EMV 3DS is available to use via Cardnet – click here to access Cardnet's SCA EMV 3DS brochure.
- Plan and test authentication journey including transacting flagging and soft declines.

Acquirer

- Discuss which exemptions may apply.
- Apply for any applicable exemptions with Cardnet.
- Plan ongoing fraud monitoring with Fraud Tool provider and Cardnet.

Website or App

- Ensure Website / Mobile optimisations testing usability and placement of payment and authentication pages.
- Prepare and display correct consumer guidance e.g. MITs, recurring payments.
- Test end-to-end cardholder journey.

I still have further questions – who do I contact?

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

- UK Finance SCA FAQs
- UK Finance Strong Customer Authentication (SCA) guidance document
- Ensuring UK SCA compliance and minimising customer impact
- Strong Customer Authentication: Communication on improving outcomes from 3D Secure – Data Consistency
- SCA UK implementation and ramp up plan

Both Mastercard and Visa have SCA guidance via their websites. Both Card Schemes also hold regular webinars on the topic of SCA. We recommend you contact your scheme representative if you do not have access to these events.

Lloyds Bank Cardnet has set up a dedicated mailbox for any further questions on Strong Customer Authentication: CardnetSCAQueries@lloydsbanking.com

lloydsbankcardnet.com

Call us:

New Customers on 0800 274 5210
Lines open from 9am-5pm Monday to Saturday

Existing customers on 01268 567 100
Lines open from 8am-9pm Monday to Saturday

Please contact us if you would like this information in an alternative format such as Braille, large print or audio.

If you have a hearing or speech impairment and would prefer to use a Textphone, call us on 0345 300 2281 (lines open 24 hours a day, seven days a week).
If you are deaf and prefer to use BSL, then you can use the SignVideo service available on our website lloydsbank.com/signvideo

Please remember we cannot guarantee the security of messages sent by email.

Lloyds Bank plc, Registered Office: 25 Gresham Street, London EC2V 7HN. Registered in England & Wales no. 2065. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority under Registration Number 119278.

Lloyds Bank plc is covered by the Financial Ombudsman Service (FOS). Please note that due to FOS eligibility criteria not all business customers will be covered.

This information is correct as of September 2021.