

COMMERCIAL BANKING



Maximise your payment acceptance

Strong Customer
Authentication and
EMV 3-D Secure



LLOYDS BANK



Contents

Introduction	3
More choice	4
What does this mean for you?	6
Important information	8



Introduction

Lloyds Bank is committed to ensuring all customers are compliant with the new standards and are able to accept as many payments as possible. The new 3-D Secure standard becomes enforceable next year and will aim to reduce fraud and ensure the cardholder journey is secure and straight forward.

It brings a new approach to tackling fraud and improving authentication via a multitude of additional capabilities; resulting in an improved online experience for your consumers and increasing transaction acceptance for your business.

Lloyds Bank welcome the FCA's decisions to move the regulatory enforcement date for Strong Customer Authentication (SCA) by a further 6 months to 14th March 2022, allowing Merchants further time to prepare. Merchants may still start to see some soft declines on non-secure or incorrectly flagged transactions from the 1st June 2021 as card Issuers start to increasingly select higher risk transactions to be authenticated with 3DS or flagged with the appropriate exemption.

You may have read our FAQ document and feel unsure if your business should switch over to utilising EMV 3DS yet. Apart from meeting the SCA compliance under PSD2, there are numerous benefits to EMV 3DS that your business could be benefiting from today. EMV 3DS addresses many of the issues inherent with 3DS 1.0 – such as poor consumer experience on mobile devices, limited data shared with Issuers and reduced security through the use of static passwords.

Why Lloyds Bank

Lloyds Bank is part of Lloyds Banking Group, who sit at the heart of the UK payments landscape. With a significant share of UK payments passing through our systems, we are provided with meaningful insights into payments activity across all channels. These insights leave us well placed to ensure we have the best set of solutions available to meet the needs of UK businesses.

We provide a full range of secure and compliant Omni Channel Payment solutions supporting your customers payment needs and expectations across all channels including face-to-face, online, mobile, and remote (customer not present) settings. This includes payment acceptance via an array of traditional and alternative payment types and wallets.

Whatever situations or channels you need to operate in we can provide a solution that will enable you to meet the payment expectations of your customers in a way that meets the needs of your business.



Please speak to us

to explore your options to improve your consumer journey and ensure your website is secure, compliant and easy to purchase through.

lloydsbankcardnet.com



More choice

Are your transactions currently processed without any authentication?

All transactions must be compliant with SCA by 14th March 2022, so will need to be switched over to EMV 3DS before this date, or flagged as exempt (see more detail in our [FAQs](#)).

By switching your transactions to authenticate via EMV 3DS, should the payment subsequently be disputed as fraudulent, the liability will usually shift from the Merchant to the Card Issuer. This could have a significant impact on your business' chargeback and liability volumes.

EMV 3DS has been built with mobile payments in mind

The improved design dramatically increases the consumers experience on mobile devices by being fully compatible with mobile wallet applications and in-app transactions.

Merchants using 3DS 1.0 often find consumers are unable to view the 3-D Secure authentication page on their device, often leading to abandoned transactions.

Does your business operate a Mobile APP?

EMV 3DS has a Software Development Kit (SDK) component, which enables comprehensive integration with mobile apps. This will make it much easier for you to integrate EMV 3DS into your app.

With the option to complete biometric authentication in some instances, whilst still in the app, your consumers will enjoy a friction-free experience through the checkout process.

Higher acceptance on your Ecommerce transactions

If you use 3DS 1.0 already, you will understand that a small volume of transactions suffer abandonment or decline at the authentication stage. As already mentioned, abandonment is reduced via mobile optimisation. According to Visa, the enhanced 3-D Secure protocol (EMV 3DS) will reduce abandonment by 70% and checkout times by 85%.

Checkout times will be improved as EMV 3DS has ten times the amount of data fields compared to 3DS 1.0. You the Merchant, can utilise these fields to provide the Card Issuer with better data; which in turn leads to a more educated decisioning process at the authentication stage. This could lead to a lower challenge rate to the Cardholder, so less requirement for two factor authentication.

EMV 3DS is a protocol and the schemes Visa and Mastercard have developed products based on this standard, Mastercard Identity Check and Visa Secure. Other schemes have developed their own solutions to support businesses to meet Strong Customer Authentication Requirements.

Discover Network including Diners Club International have developed ProtectBuy. American Express offer a product called Safekey.

Should a Business wish to accept these card types via their website or App based payment services as with EMV 3DS access to these additional authentication protocols is required.

Lloyds Bank payment services are able to support these additional schemes should you wish to expand your acceptance methods.



Could your business utilise Non-Payment Authentication?

EMV 3DS has the additional ability to complete Non-Payment Authentication. This is where you have the ability to authenticate the Cardholder without them making an immediate purchase.

This functionality could be very useful if your business needs to add cards to e-wallets, for example storing a card on file for later use.

Does your business complete Merchant Initiated Transactions (MITs)?

If you have read the [FAQ](#) document, you will know that 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 3DS cryptogram, this will provide evidence to the Card Issuer that the first transaction has completed card holder two factor authentication.

As the first transaction would class as a Cardholder Initiated Transaction (CIT), this would be in scope of SCA and require two factor authentication. As not all transactions that pass through EMV 3DS automatically go back to the Cardholder for two factor authentication, EMV 3DS is vital as this provides the Merchant with the ability to force a mandated challenge field to the cardholder.

Merchants should make sure they have tested this with their end-to-end consumer journeys in advance of the deadline so that they do not see transactions fail.



Transactions processed by Apple Pay and Google Pay already adhere with SCA 2 factor authentication requirements.

Offering a greater choice of alternative payment methods such as digital wallets can result in lower shopping cart abandonment. Lloyds Bank can support you with choosing the right payment types for your business.



What does this mean for you?

When do I need to be ready?

Lloyds Bank recommends adopting the most up-to-date version, EMV 3DS Version 2.2 as soon as possible. UK Finance have confirmed that from 1st June 2021, Card Issuers from all UK banks will start to sample a percentage of transactions to test readiness.

Card Issuers may decide to soft decline unsecure transactions of those being incorrectly flagged. The soft decline means the issuers want more information to continue the transaction and is asking you the Merchant to go back to the Consumer and ask them to apply two factor authentication.

As we have already mentioned, in a 3DS 1.0 journey via a mobile device, this is often clunky with the consumer not understanding the request or sometimes not being able to view the request at all.

This mirrors the roll out in the majority of Europe where soft declines were also used to ensure SCA readiness as the enforcement date in the rest of the EEA was 31st December 2020, therefore if you accept EEA issued cards you may already have experienced these soft declines.

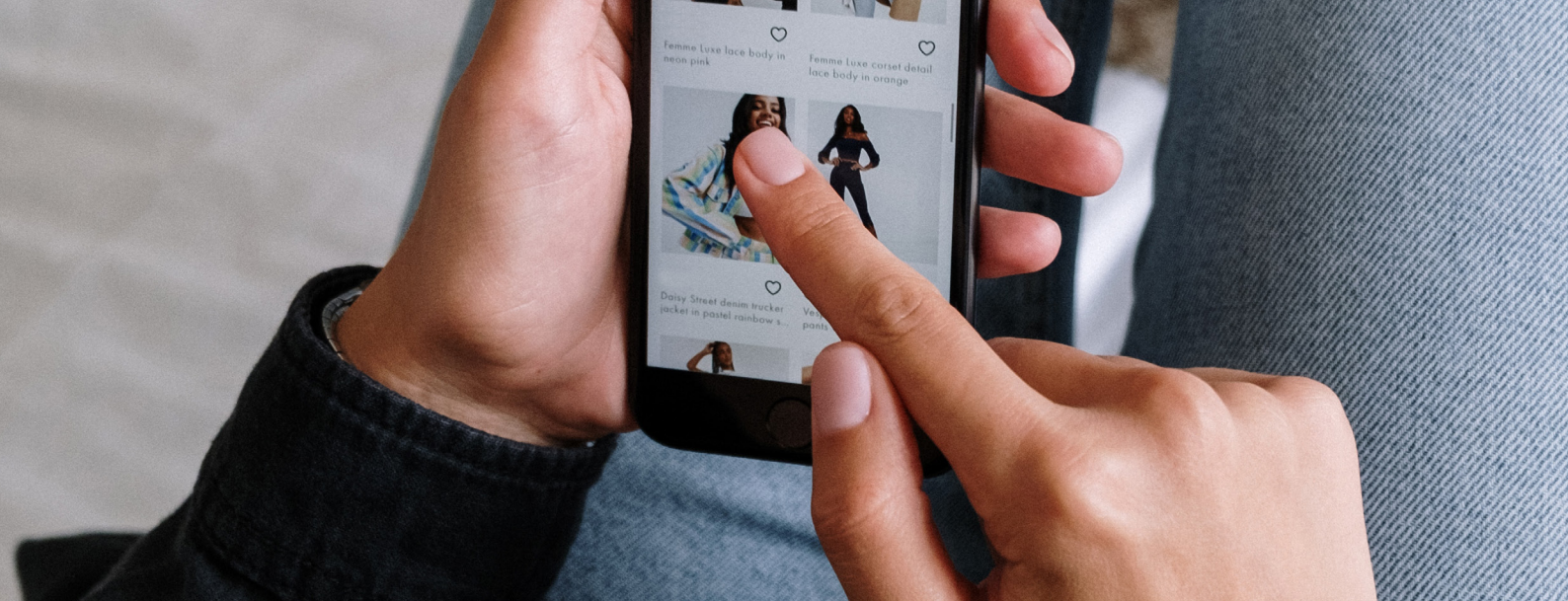
Do you want to apply exemptions such as Low Value or Transaction Risk Analysis (TRA) to transactions?

In some circumstances, there may be an exemption that can be applied to specific online payments which may reduce the requirement for two factor authentication. For information on exemptions, please read our [FAQs](#).

If your business has discussed this with Lloyds Bank and confirmed that you are permitted to apply exemptions to some of your Ecommerce transactions, 3DS version 2.2 is already a necessity. This is the version of 3DS required to flag your transactions correctly through to authentication.

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 16 th Oct 2021 (VBN AI09869 on VOL, subject to issuer participation) Mastercard: Currently offers liability, withdrawal date 14 th 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



Exemption flagging is not possible in 3DS 1.0. Even if you wish to send flagged transactions straight to authorisation, bypassing authentication completely, a Card issuer can still disregard this exemption with a soft-decline and request customer authentications.

This will then require you as the Merchant to request, via the 3-D Secure message, that two factor authentication is required by using the mandated challenge flag. The mandated challenge flag is only available in EMV 3DS.

How will I know when to send a transaction via 3DS?

Lloyds Bank's Payment Gateway solutions automatically trigger EMV 3DS.

We also offer solutions which allow you to set rules and apply exemptions at merchant level. This gives you flexibility to determine how to apply SCA and the correct level of authentication for each transaction based on the desired parameters.

If you use a third party payment service provider, we advise you to discuss your business authentication requirements to ensure a compliant solution is tested and in place before the 1st June 2021 ramp-up date.

Additional cost impacts of utilising 3DS 1.0

Effective 29th December 2020, Mastercard have doubled the existing 3DS 1.0 Authentication Transaction Fee to €0.04.

Do I still need a fraud tool when SCA regulation starts?

Whilst many merchants and consumers alike wish to have the simplest way to pay, the new mandated SCA/EMV 3DS requirements which come into force in the UK on 14th March 2022, enhance the protection to consumers and provides consumers with the confidence that they are doing business with a credible merchant that takes card payment security seriously. Extending this protection into a well-integrated fraud management tool will be transparent to the consumer, but will help protect merchants from potential brand reputational damage,

wider fraud attacks and mitigate financial losses from any fines imposed from regulatory bodies.

Whilst a successfully authenticated EMV 3DS transaction provides fraud chargeback protection for the merchant, it cannot prevent chargebacks initially being raised and having to subsequently be challenged, for a variety of reasons available to the consumer by their card issuing bank. This is why a layered approach to fraud management and security should be implemented, not just to protect against fraudsters but also to protect your genuine cardholders whose details may be being targeted by those fraudsters via other channels or online accounts with stored card credentials. Lloyds Bank are able to work with your business to assess which of our fraud tool options would be the most appropriate for managing the fraud risk for your Business.

Does SCA impact consumers who pay via the PayFrom Bank option at checkout?

Powered by the Open Banking revolution, your business website or app can increase its payment acceptance to include payments directly from your customers' bank accounts. Lloyds Bank PayFrom Bank is a payment method available to payers in the United Kingdom that allows them to purchase or pay for goods and services using direct online transfers from their bank. Banking apps utilise two-factor authentication to log in and confirm payments, therefore allowing your business to be confident that SCA requirements are being met and that the payment is secure and compliant. Lloyds bank can talk with you about your payment acceptance methods and which ones may be beneficial for your business and customer base.

Our Strong Customer Authentication **FAQ** document includes links to helpful UK Finance Guidance and Scheme information. To find out more about the solutions Lloyds Bank can offer you to support your SCA compliance, please [contact us](#).



Go to 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

Important information

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

Cardnet® is a registered trademark of Lloyds Bank plc.

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 January 2021.



LLOYDS BANK