UK Finance communication on requirements for Strong Customer Authentication

Date: September 2020

What is Strong Customer Authentication (SCA): A new set of rules that will change how consumers confirm their identity when making purchases online.

When does it apply: The rules apply in full for card payments, from 14 September 2021 in the UK and from 31 December 2020 in the rest of the EU. These deadlines will not change.

When is SCA readiness required: Parties engaged on e-commerce card based payments need to enable all SCA flows by 31 May 2021 in readiness for the UK SCA Ramp up

Why does it matter to you: If you do not take action, e-commerce card-based payment transactions that are non-compliant will be declined. Implementation of these new rules may require testing and specific changes to your payment process. We therefore encourage you to take immediate action to ensure you are not at risk of declined transactions which may impact your business.

What should you do: Urgent action should be taken by businesses with an online presence. You should contact your payment provider such as your acquirer or gateway to discuss the implementation.

Call to action: This communication provides important information for businesses of all sizes looking to avoid customers experiencing declined e-commerce transactions after the UK's Strong Customer Authentication enforcement deadline of 14 September 2021 and the EU's deadline of the 31 December 2020. After this point card issuers will begin to decline all non-compliant transactions. To avoid a cliff-edge implementation and minimise impact to customers, from 1 June 2021 UK issuers will start checking randomly if e-commerce transactions are SCA compliant and soft-declining them if not (UK SCA Ramp up). We actively encourage businesses with an online presence to read the content of this communication and to get in touch with your payment provider (otherwise known as an acquirer or gateway). This should be done with urgency due to the implementation lead times and testing period required.

What is Strong Customer Authentication?

Strong Customer Authentication (SCA) is a new set of rules that will change how consumers and business customers confirm their identity when making purchases online to help further protect them from fraud. Following its implementation, consumers shopping or banking online will often need to undertake an extra step to confirm their identity. For example, the card issuer or provider (for example a bank) may use one of a number of ways to verify a purchase or login, such as a passcode via text message, a phone call to the consumer's landline, the use of a card reader or the use of a smartphone app. Under the new rules all parties are required to make the necessary changes to enable consumers to authenticate their actions in a manner compliant with the underlying regulation.

Background:

From 14 September 2019, changes were introduced to online payments in order to provide further protection to customers. Under the Payment Service Directive 2 (PSD2), Strong Customer Authentication (SCA) is required where a payment service user (customer) initiates an electronic payment transaction.

However, in the UK the Financial Conduct Authority (FCA) provided a longer lead time for enforcement, due to the complexity of implementing SCA. At the request of the FCA, UK Finance established a Programme Management Office (PMO) to coordinate the UK industry managed roll-out plan agreed in the summer of 2019. The European Banking Authority (EBA) similarly allowed for regulatory flexibility on enforcement[1] until 31 December 2020. The aim was to ensure all parties moved towards full compliance in an orderly manner, thus avoiding negative impacts for both consumers and merchants.

In light of the impact of Covid-19 on key stakeholders, and to minimise the impact on both consumers and e-merchants, the FCA has updated its Strong Customer Authentication page with a revised date of 14 September 2021 for the implement strong customer authentication (SCA) for e-commerce. This can be found here.

Therefore, the new enforcement date is 14 September 2021 in the UK1 and 31 December 2020 across the rest of the EU. As a result, UK card issuers will be required to decline all non-SCA-compliant transactions after 14 September 2021. However, UK issuers will start randomly checking if ecommerce transactions are SCA compliant from 1 June 2021 and soft-declining them if not.

All merchants, acquirers, gateways, and issuing banks or payment service providers must be ready to support SCA from 1 June 2021, to avoid the risk of consumers experiencing declined e-commerce transactions. The FCA has confirmed that there will be no further extensions to this deadline. In order to avoid a loss of business, we encourage all parties to read this communication and to take action.

This communication sets out what is required, and by when so that you can be ready for this change. For more information on the UK SCA Implementation plan click here.

What does SCA require?

SCA will be required for all online (website or app) card-based payments, unless one of the limited exceptions or exemptions[2] allowed under the rules can be applied. For card payments this means **all e-commerce transactions that are unable to be authenticated or those without exemptions will be declined after 14 September 2021.**

For e-merchants, this means you will need to work with your acquirer or gateway to ensure you upgrade your payments process to support a technology called 3DSecure, in order to be able to cater for the new requirements. This often requires a testing process and potentially testing slots, so you should engage as soon as possible to avoid further delays as SCA readiness is required by 31 May 2021 due to the UK SCA Ramp up.

For further details, please refer to Appendix Table 1 – SCA E-commerce Compliance for the definition of SCA compliant versus non-compliant transactions.

If I am a merchant/business with an online presence what do I need to do?

You need to speak to your payment providers (e.g. acquirers, gateways) and, where relevant, your trade associations, to understand the steps you need to take in order to prepare and meet the agreed timeline, including understanding:

a) which version of 3DSecure to use (the technology which enables SCA)
b) which exemptions you might be able to use to encourage a better customer experience, and how to use these
c) correct flagging (exemptions or out of scope) of transactions sent directly to authorisations
d) Soft-decline support (if applicable)
e) dates and windows for testing your checkout process/website

---

[1] EBA opinion issued in October 2019 provided for enforcement of the new rules to start after 31 December 2020. Most member states have aligned to this deadline.

[2] Please refer to the Regulatory Technical Standards on strong customer authentication and common and secure open standards of communication or UK Finance's upcoming guidance for more information about SCA exceptions and exemptions.

f) date for go-live.

E-merchants are encouraged to understand their plans as soon as possible due to the amount of change that might be required and the potential negative impact if no action is taken.

Who does this apply to?

The FCA decision not to take enforcement action from 14 September 2019 was based on the commitment that everyone that needs to will take timely, meaningful and necessary steps towards compliance. Failure to do so will subject Payment Service Providers (PSPs[3]) to full FCA supervisory and enforcement actions as appropriate. Failure to act by all participants in the ecosystem will result in declined e-commerce transactions – therefore it is vital everyone takes the required steps as soon as possible to ensure readiness by 31 May 2021 for the UK SCA Ramp up scheduled ahead of the enforcement deadline of 14 September 2021.

The key aim is to minimise any customer impact by avoiding a cliff-edge implementation by the enforcement deadline. This means all parties in the ecosystem need to ensure all necessary preparations are completed before the end of May 2021.

If I am an acquirer or gateway what do I need to do?

Acquirers and gateways should work actively with e-merchants to ensure they are working towards operational readiness in advance of the deadline. Acquirers and gateways should be tracking e-merchant progress and actively reaching out to those that have not yet taken action.

Acquirers should work with gateways to obtain a clear plan for 3DSecure version 2.1 or v2.2 and how they will enable e-merchants to accelerate towards operational readiness in line with scheme mandates. We look to both schemes and acquirers to evidence certifications of 3DSecure version 2.1 and v2.2.

If I am an issuer what do I need to do?

In alignment with reporting requirements issued in October 2019, issuers and acquirers are expected to confirm with the FCA their ability on a bilateral basis to accept and process 3DSecure v2.1 (or higher), their handling of exceptions or exemptions and their path to reduce reliance on text based one-time passcodes (SMS OTP), as well as ways to support vulnerable customers.

As the market moves towards completion of testing, issuers should begin to enable SCA gradually from February 2021 to allow consumers and e-merchants to adapt to the change. Please refer to the UK SCA Issuer led Ramp up materials for detailed information.

How can I achieve operational readiness?

For card payments, the common industry practice to facilitate Strong Customer Authentication is something called 3DSecure (3DS[4]). This technology is also required in order to facilitate the use of SCA exemptions and enable SCA when needed. There are currently three main versions of 3DSecure on the market. Versions 2.1 and 2.2 are summarised below.

- 3DSecure version 1.0
- EMV 3DSecure version 2.1[5]
- EMV 3DSecure version 2.2[5]

---

[3] In the context of PSD2, Payment Service Providers (PSPs) are Issuers and Acquirers.

[4] EMV Three-Domain Secure (3DS) is a messaging protocol developed by EMVCo to enable consumers to authenticate themselves with their card issuer when making card-not-present (CNP) e-commerce purchases. The additional security layer helps prevent unauthorised CNP transactions and protects the merchant from CNP exposure to fraud. The three domains consist of the merchant / acquirer domain, issuer domain, and the interoperability domain (e.g. Payment Systems).

[5] Mastercard has developed 3DS message extensions which are applicable to 3DS2.1 (3DS2.1. with merchant extensions) and 3DS2.2 (3DS2.2 with merchant extensions). This message extensions will facilitate the usage of SCA exemptions via 3DS2.1. Please refer to the Appendix – Table 3 for more information

Visa, Mastercard and American Express have set up respective issuer and acquirer mandates for the different 3DSecure versions to encourage the adoption of versions 2.1 and 2.2.

- **EMV 3DSecure Version 2.1** was enhanced in response to the new SCA fraud and security requirements, as well as the ability to adapt to in-app payments and to authenticate a card transaction through a mobile banking app. Biometric authentication might be supported via the issuer's mobile banking app if they choose to offer this. Version 2.1 also has enhanced the ability to respond to other new requirements such as "soft declines".

- **EMV 3DSecure Version 2.2** builds on the foundation of version 2.1 by providing consumers with an improved consumer experience for mobile banking app authentication, as well as adding the support for embedded biometric authentication methods such as fingerprints and facial recognition. Additionally, version 2.2 also provides support for exemptions via authentication, as well as useful features for more complex use cases.

If you are unable to move onto version 2.1 or 2.2 by the 31 May 2021 deadline (UK SCA Ramp up), 3DSecure version 16 can still support SCA, but is more limited as it does not support the new, more secure authentication methods such as mobile banking app or embedded biometrics nor SCA exemptions via authentication. It is also important to note that, due to the limitations, more transactions via this route are likely to fail or be declined.

The use of acquirer SCA exemptions called transaction risk analysis (TRA) and low value can be supported by issuers via authorisations directly (rather than via authentication through 3DSecure). So regardless of the 3DS version supported, you can still utilise applicable acquirer exemptions if your transactions go to 'via authorisation' directly. E-merchants are encouraged to speak with their acquirers to find out more about acquirer SCA exemptions.

Please refer to the Appendix – Table 2 and Table 3 for more information about the different versions of 3DSecure.

Our next steps:

UK Finance will continue to work with the industry to track progress against the agreed delivery plan. Further detailed guidance, including the timelines for interim milestones as well as coordinated testing and live-proving support will be shared later in 2020.

For further details on the EBA opinions and other UK Finance Programme Management Office (PMO) updates, please visit our website here.

[6] American Express supports exemptions in all 3DS versions. Please talk to your American Express representative for more information.

Appendix

Table 1: SCA E-commerce Compliance (applicable as of 1 June 2021 – UK SCA Ramp up)

- Includes in-scope e-commerce card-based payment transactions only (excludes mail and telephone order, one-leg-out and merchant-initiated transactions (MIT))
- Although MIT is out of scope, the first transaction (recurring payment set up) requires step up to Strong Customer Authentication. Therefore, references to MIT are made within the table below

	Via 3DSecure	Directly to Authorisation
Compliant Transactions	• Transactions with an acquirer exemption flag (Acquirer TRA) • Transactions sent for issuers to step up (SCA) or use an issuer exemption (TRA, low value or trusted beneficiary flag) • Recurring payments set up (1st transaction) request for an issuer step up (SCA to be applied)	• Transactions flagged with an acquirer exemption flag (Acquirer TRA, low value) • MIT transactions with the relevant Auth Code or Transaction ID generated during recurring payments set up (1st transaction) – ***This process will allow MIT transactions to be recognised as out of scope***
Non-Compliant Transactions	**Note:** all in scope transactions need to be sent via 3DS unless they are sent directly to authorisation with an acquirer exemption flag	• Transactions sent directly to authorisation with no acquirer exemption flag • MIT transactions with no Auth Code or Transaction ID

Table 2: Visa, Mastercard and American Express 3DS Scheme Mandates

	Issuer mandate			Acquirer mandate		
	Visa	**Mastercard**	**American Express**	**Visa**	**Mastercard**	**American Express**
3DS2.1	**14 March 2020**	**April 2019 (no enforcement action taken to date)**	**TBC**	**N/A**	**April 2019 (no enforcement action taken to date)**	**TBC**
3DS2.1 with message extensions	**N/A**	**July 2020**	**N/A**	**N/A**	**July 2020**	**NA** **Not supported**
3DS2.2	**14 September 2020***	**No mandate in place**	**TBC**	**16 October 2020***	**No mandate in place**	**TBC**
3DS2.2 with message extensions	**N/A**	**July 2020****	**NA** **Not supported**	**N/A**	**July 2020****	**NA** **Not supported**

*Visa issuers and acquirers have been offered a waiver extension to their respective EMV 3DS 2.2 mandate dates until 14 March 2021 so long as they are fully enabled on EMV 3DS 2.1.

**Mastercard currently have no mandate for 2.2 but if 2.2 is used then you this must be used with extensions to allow the use of exemptions

Table 3: 3DS – Considerations when choosing a version to support

3DS Version	3DS1	3DS2.1	3DS2.2
Journey optimised for mobile and tablet devices	x	✓	✓
A choice of authentication options can be provided to customers during check out (authentication methods to be defined by issuers)	x	✓	✓
TRA exemption can be applied by Issuers	✓	✓	✓
TRA exemption can be applied by Acquirers**	x	x	✓
Customer journeys with delayed shipment/delivery (post 90 days) are supported (no need for re-authentication using SCA)	x	✓	✓
MIT set up can be flagged and recognised by issuer. Therefore, customers do not need to be authenticated for MIT series	x	✓	✓
Trusted beneficiary exemption support (if offered by issuer)	x	x	✓
Delegated authentication support	x	x	✓

* 3DS v2.1 plus extensions will support most of the functionality of 3DS2.2
** Acquirers can apply TRA exemption directly via authorisations regardless of the 3DS version being used