What is Strong Customer Authentication?

Strong Customer Authentication (SCA) is a European regulatory programme which focuses on increasing the security of online payments. By September 2019, 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. Mastercard have mandated that these changes are implemented by April 2019, and Visa by September 2019. 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 it impacts 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?

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 €100 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 is not required for transactions where the fraud rate of your Payment Service Provider is below the thresholds shown below.*

Trans Value	***Gross Fraud Rate***
<=€500	*0.01%*
<=€250	*0.06%*
<=€100	*0.13%*

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

Whitelisting - 2 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. 2 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 2 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 will be some changes to the contactless counters, however these will be managed by the Payment Service Providers and there is no requirement to update terminals. Your customers should not notice any changes as they are currently required to step up authentication to Chip and PIN when current counters are reached.

Can I apply these exemptions?

It is down to each Issuer and Acquirer to decide whether or not any of the exemptions can be applied. There is no legal requirement for an Issuer or an Acquirer to offer these to their customers. Cardnet are currently working through their strategy for the application of exemptions.

What do I need to do for 1st April 2019?

To comply with the SCA requirements and to ensure the best possible cardholder experience MasterCard have developed version 2.0 of their secure code product. This has been re-named identify check. At the moment, most merchants use version 1.0, however by 1st April 2019, MasterCard have instructed that all online payments need to be processed using version 2.0.
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.

What do I need to do for 14th September 2019?

Visa need you to use version 2.0 of their secure online product Verified by Visa. 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 the technical changes you may be required to make.

What will happen to my transactions after 1st April 2019 if I do not make any changes?

You need to ensure that all development required on your website is completed by your web development team by this time. If the updates are not carried out in time, there is a possibility that e-commerce transactions will not be processed.

What will happen to my transactions after 14th September 2019 if I do not make any changes?

Issuers may decide to decline non-compliant transactions.

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 liable for fraud*

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