What Do I Need to Do to Be SCA Compliant?

In January 2018, the second Payment Services Directive (PSD2) came into force. This was introduced to increase consumer protection, improve payment security and prevent fraud. From 14 September 2019, PSD2 requires payments to be validated using Strong Customer Authentication.

What's Strong Customer Authentication (SCA)?

All electronic payments, whether face to face or remote, require SCA. This means a customer must authenticate their payment using at least two independent factors:

Possession – something only you have. For example, your mobile device registered with your issuing bank or a hardware token that has been issued to you

Inherence – something only you are. For example, your fingerprint, iris scan or other form of biometric that can uniquely identify you.

Knowledge – something only you know. For example, a unique passphrase or identification number this is known only to you.

Further information on PSD2 and SCA can be found within our Blog section. You'll find our whitepaper called 'The changing face of card payments' and our blog called 'Payment Services Directive 2 (PSD2)' there.

Does SCA apply to all transactions?

Chip and PIN transactions already adhere to SCA	✓
Contactless payments are exempt, however, a new decline code is being introduced that will ask the cardholder to complete a chip and PIN transaction if extra security is required (see the Face to Face Transactions section)	✗
Unattended parking and transport terminals are exempt	✗
All other unattended devices are required to support chip and PIN	✓
Mail Order and Telephone Order (MOTO) transactions, Recurring Transactions and Merchant Initiated Transactions (Stored Credential Transactions, also known as Credential on File Transactions), are out of scope for SCA but need to be flagged correctly (see the MOTO and Merchant Initiated Transaction section)	✗
Ecommerce transactions require SCA (see the Ecommerce Transaction section)	✓
Anonymous transactions (pre-paid cards) - not subject to the SCA mandate	✗
International transactions – it may not be possible for UK-based customers to apply SCA to transactions when the card issuer isn't located in the European Economic Area (EEA), but you should still attempt SCA for all transactions	✓

How's my business affected by SCA?

The changes you need to make for SCA depend on the type of transactions you process. Please refer to the following sections to see what you need to do.

Face to Face Transactions

Chip and PIN transactions already comply with the SCA requirement for two factor authentication. Your customer is in possession of their card and know their PIN.

Transactions made using a mobile device, like a mobile phone also comply with SCA as the customer is in possession of their phone, and use a fingerprint to uniquely identify themselves.

Contactless transactions don't fulfil the requirement for two factor authentication but are exempt from the SCA requirement. However, additional security requirements may be requested by the card issuer. A new decline code is being introduced that will ask the cardholder to complete a chip and PIN transaction where that extra security is required.

What do I need to do?

If you rent your terminal from us, we'll make the changes for you. Just ensure that you and your staff understand what's happening and be ready to reassure cardholders that there's no problem with their card or their account, just that it's an extra security check requested by their card issuer.

If you own or rent your terminal from another source, contact them **immediately** to discuss the decline code changes needed for the step up from a Contactless to chip and PIN transaction. Details of the technical requirements for SCA can be found in our *PSD2 and Strong Customer Authentication Technical Implementation Guide*.

MOTO and Merchant Initiated Transactions

While MOTO and Merchant Initiated Transactions (Stored Credential Transactions, also known as Credential on File Transactions, where card details are stored for future use), are out of scope for SCA, if the card issuer doesn't know they're one of these kinds of transactions, they may request SCA. If the cardholder is unable to provide the necessary authentication, the transaction will be declined.

What do I need to do?

It's critical that all transactions are flagged correctly.

If you rent your terminal from us or use our E-Commerce Platform, we've made all the necessary changes to ensure transactions contain the correct flags.

If you own or rent your terminal from another source or use a third party provider for your ecommerce service, contact them **immediately** to ensure your transactions are flagged correctly.

Further information on Stored Credential Transactions and details of their technical requirements can be found on our website within our Customer Centre under the Stored Credential Transactions tile. They'll also need to apply the technical requirements, which can be found in our *PSD2 and Strong Customer Authentication Technical Implementation Guide*.

Ecommerce Transactions

☞ Payments made via a website require SCA. These transactions must now support 3D Secure, which is the ecommerce authentication protocol by the Card Schemes, such as Mastercard and Visa. This allows the cardholder to authenticate themselves as the genuine holder of the card. Under PSD2, card issuers are obliged to challenge and potentially decline transactions that don't comply.

A new version of 3D Secure (3D Secure 2 – 3DS2) is being introduced to comply with new regulations and provide a better customer experience, more security for your business and a frictionless payment experience. Read our blog called '3D Secure 2 – A Beginner's Guide'.

What do I need to do?

If you use our Global Payments E-Commerce Platform (previously Realex Payments), this will support 3DS2 from September 2019. You should have already received communications from us about the changes you need to make to comply with the new SCA requirements. . If you've any questions about the changes or would like more information on our E-Commerce Platform, please email ecomsupport@globalpay.com.

If you use a third party provider for your ecommerce services, you need to review the way in which you accept card payments. Please speak to your solution provider to make sure your solution is up to date with all the flagging requirements and that they're making changes for the SCA mandate. Our 3DS2 solution may be used alongside your existing gateway solution, if required. You can contact us on the email above for help with this.

Details of the technical requirements for SCA can be found in our *PSD2 and Strong Customer Authentication Technical Implementation Guide*.

Ready to Get Started?

- ☐ Remember, these changes are being made to increase consumer protection, improve payment security and prevent fraud, which will benefit your business
- ☐ Read the information we've provided on our website to help understand what the SCA requirements are
- ☐ If you own or rent your terminal from another source or use a third party provider for your ecommerce service, contact them **immediately** to ensure they're making the necessary changes and share our technical docs with them

We know that these changes can be confusing, so there are answers to some questions we think you may have in our FAQs. We also have a SCA Decision Tree.

Take a look at these and if you have any other questions, or you want to talk to someone about how SCA affects your business, please call your Relationship Manager or our helpdesk on 0345 702 3344*, selecting the option for 'all other enquiries'.

*Lines are open between 9am - 6pm Monday to Friday, excluding public holidays. To help us continually improve on our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recordings remain our sole property. We also provide a Textphone service on 0345 602 4818.