Strong Customer Authentication (SCA)

What is Strong Customer Authentication?

Strong Customer Authentication (SCA) is a new European regulatory requirement to reduce fraud and make online and contactless offline payments more secure. To accept payments and meet SCA requirements, you need to build additional authentication into your checkout flow. Strong Customer Authentication requires authentication to use at least two of the following three elements:

- **Knowledge** (Something the user knows. For example, password or PIN).
- **Possession** (Something only the user possesses. For example, a phone or hardware token).
- **Inherence** (Something the user is. For example, fingerprint or face recognition).

(To find out more about the original Strong Customer Authentication requirements, consult the Regulatory Technical Standards (RTS).

Banks will need to start declining payments that require SCA and don't meet these criteria. Although the regulation was introduced on 14 September 2019, we expect these requirements to be enforced by regulators over the course of 2020 and 2021.

When is Strong Customer Authentication required?

Strong Customer Authentication applies to "customer-initiated" online and contactless offline payments within Europe. As a result, most card payments and all bank transfers require Strong Customer Authentication. Recurring direct debits on the other hand are considered "merchant-initiated" and don't require strong authentication.

For online card payments, these requirements apply to transactions where both the business and the cardholder's bank are located in the European Economic Area (EEA).

What are Strong Customer Authentication exemptions?

Under this new regulation, specific types of low-risk payments may be exempted from Strong Customer Authentication. Payment providers are able to request these exemptions when processing the payment. The cardholder's bank will then receive the request, assess the risk level of the transaction, and ultimately decide whether to approve the exemption or whether authentication is still necessary.

> Merchants should contact their Acquirer before managing their own exemptions.

Strong Customer Authentication exemption scenarios

Low-value payments

Transactions under €30 and cumulative payments higher than €100 on the same card.

Transactions under €30 EUR are exempt from Strong Customer Authentication. However, the issuing bank will keep track of how many payments are made using this exemption.

Strong Customer Authentication is required if the total amount attempted on the card is higher than €100 EUR, and every five transactions.

Acquirer Transaction Risk Analysis

Transaction Risk Analysis, as outlined by the Regulatory Technical Standard (RTS), looks at risk scores and other account risk factors to confirm that no abnormal spending or behavioral patterns of the payer have been identified.

Under PSD2 SCA, TRA exemptions can be applied at either the acquiring or issuing side of the transaction.

Trusted beneficiary exemption

Certain trusted merchants chosen by the cardholder

Customers can assign businesses to a whitelist of ‘Trusted Beneficiaries’. This list is maintained by their bank. Whitelisted merchants, whatever the transaction amount, can be exempt from Strong Customer Authentication.

This lets regular customers mostly skip Strong Customer Authentication with the businesses they've chosen to whitelist.

Secure Corporate Payment (SCP) exemption

Payments between corporations

Payments made between two corporations can be exempt from Strong Customer Authentication. But, this is only possible when the payment method is a payment instrument dedicated to making such B2B payments.

Merchant Initiated Transaction (For Mastercard only)

Transactions without direct customer involvement

Merchant-initiated transactions (MITs) are transactions that don't directly involve the customer. The payment is taken from a saved card with the customer’s prior consent on an arranged date.

For example, some products have a variable cost based on usage, like energy contracts. The first payment, or the first time the card is saved, always needs to be authenticated. But the following payments can skip Strong Customer Authentication if marked as a 'Merchant Initiated Transaction'.

Recurring transactions are only an exemption for Mastercard. Visa does not accept this use case as an exemption but sees it as out of the scope of PSD2 and hence out of the scope of Strong Customer Authentication, so authentication will not be required. For MITs (CHARGE), CIT (SIGNUP) needs to be performed in advance, with appropriate Strong Customer Authentication, to establish the initial agreement with the cardholder. This CIT (SIGNUP)may be a zero-value transaction.

Strong Customer Authentication Delegation

Delegated authentication

In the traditional payment flow, authentication is carried out by the issuer. Delegated authentication means that the merchant can directly authenticate the customer, skipping the redirection to the issuer and facilitating the 'one-click purchase' experience.