SCA Best Practice Guide
Merchants & Payment Gateways

New EU and UK regulation starting 2021

Is your checkout optimised for PSD2 SCA?

What you need to know:

1. As of 1st January 2021, Strong Customer Authentication (SCA) – also known as two-factor authentication – is mandatory for all European digital payments, even from within the United Kingdom.

2. To comply with the regulation, banks must decline certain payments if they don't use SCA. This means not using SCA could result in increased levels of declined card-not-present (CNP) transactions which can create customer dissatisfaction and impact your sales.

3. To avoid business disruption, confirm that you meet the new requirements for authenticating online payments – or start the process to add SCA to your checkout now.

Act now to ensure SCA-readiness: contact your acquirer

- ✓ Request information on how they will help you get ready and what you need to do to support SCA
- ✓ Discuss your other payment methods (some meet SCA requirements, so there may be no need to change everything)
- ✓ Take time to test the new authentication flow to ensure everything is running smoothly in advance of the compliance deadline. Ask your acquirer how they can help via the Mastercard merchant testing facility.

If executed well, SCA helps reduce fraud and false declines of CNP transactions while providing an enhanced checkout experience

What is Strong Customer Authentication?

It's a new European (and UK) regulatory requirement to make digital payments more secure. To ensure SCA readiness and continue accepting digital payments, you must include additional authentication into your checkout.

SCA means authentication based on the use of two or more independent elements, also referred to as factors, which are categorised as 'knowledge', 'possession' or 'inherence'.

Knowledge
Something only the cardholder knows, e.g. pin, password, secret fact

Possession
Something only the cardholder has, e.g. mobile phone, token

Inherence
Something only the cardholder is, e.g. face recognition, fingerprint

Are there any transactions not requiring SCA?

Yes, there are a number of exemptions that negate the need for SCA on certain transaction types, e.g. low-value payments (**equal/below €30**, but conditions do apply), repetitive transactions (same value) or transactions to trusted merchants.

Exemptions are defined by PSD2's **Regulatory Technical Standards (RTS)** and are always at the discretion of banks and/or acquirers. Hence, it is important to be ready to use SCA and Mastercard Identity Check to reduce the risk of declined transactions after December 2020.

The EU date for SCA compliance **is 31st December 2020**, and in the UK **14th September 2021**. If your business supports transactions from anywhere within the UK or the EU, you are advised to support SCA by the 31st December 2020 to avoid the risk of declined transactions.

How is Mastercard helping with these changes?

mastercard. ID Check

Mastercard® Identity Check™ is the solution for all Mastercard cardholders to the requirements of PSD2 and SCA. It leverages EMV® 3-D Secure – a global industry standard allowing merchants to send richer data to issuers during a CNP transaction. The result is reduced CNP fraud and abandonment rates, improved approval rates and a smoother customer experience.

Your benefits include:

- ✓ **Seamless integration** into your checkout process
- ✓ **Enhanced security** through dynamic passwords and biometric authentication
- ✓ **Greater flexibility:** Identity Check supports Credential-on-File (COF) and tokenization, and works for mobile and in-app payments
- ✓ **Smooth checkout:** smarter decision-making with 10x the data exchanged

You'll have to make the change at some point – and the sooner you do, the more secure your business will be.

Test your checkout with Netcetera and Mastercard

To get your checkout ready for SCA and EMV® 3-D Secure 2.x, we've collaborated with Netcetera to test and eliminate errors before your peak shopping season. Part of our Mastercard® Identity Check™ solution mandate is that 3DS 2.x error rates be below 1% (Authentication Guide for Europe, Authentication Best Practices).

How it works

You must be enrolled with Mastercard Identity Check to register for Netcetera's EMV 3DS Testing Platform. There are 19 different tests, including different channels, methods and exempt payments.

Refer to the Merchant Test Result Matrix for details on test cases, scenario description and flagging, test card numbers, and PASS criteria.

1

Register for the EMV 3DS Testing Platform*

- Have your merchant ID and acquirer BIN* to hand, as they are mandatory fields. After registering, click the verification link emailed to you within two hours to activate your account.
- Please read the User Guide for the Mastercard PSD2 Merchant Testing.

2

Use the 3DS Testing Platform

- Complete each test case, with your website or app-based shop, using test card numbers provided by us.
- If you have questions, please contact Mastercard with your registered merchant ID and Acquirer BIN.

*By registering, you agree to the Privacy Policy regulating the rights for processing the registration data you have provided.

Best practices

To ensure an easy transition, we encourage you and your acquiring bank to follow certain best practices:

1. Your Merchant Name

The merchant name in authentications must uniquely identify the merchant in all countries where it operates for all its activities (e.g. Merchant.com), per its activities (e.g. MerchantBooks.com), or per its countries (e.g. Merchant.co.uk).

Acquirers must ensure the given merchant name belongs to the merchant and is registered for use in the Identity Check programme.

2. Merchant enrolment *

Many EMV 3DS authentications are rejected by the Directory Server (error 303) because the merchant ID and acquirer BIN combination is not properly enrolled in Identity Check via the Identity Solutions Services Manager (ISSM) tool. It is important that merchants:

1. ensure they are enrolled by their acquirer
2. provide the correct combination (Acquirer BIN, Merchant ID) to their 3DS Servers or gateways.

3DS Servers can also enrol merchants in ISSM, including via the API (which does not require acquirer delegation).

If a merchant is acquired by several acquirers, then all combinations of (Acquirer BIN, Merchant ID) have to be enrolled by them.

To avoid the rejection of merchant IDs, it is recommended that the acquirerMerchantID field is filled without leading zeros in authentication messages and in ISSM.

* Only Acquirer BIN, Merchant ID combinations enrolled for the Mastercard Identity Check program can send EMV 3DS authentication requests. Others will be rejected. Please ask your acquirer which Acquirer BIN / Merchant ID can be used.

3. Missing or inaccurate data in key EMV 3DS fields

Based on the fields marked as high importance, we can see the following are being used as part of authentication models:

- Device Info
- Cardholder Account Number
- Browser IP address
- Cardholder Name
- Cardholder Mobile Number
- Billing Address (also address match indicator in UK)

It's therefore important that merchants send these fields to maximise the chance at frictionless authentication and drive higher approval rates. From experience, many merchants leave data fields blank, taking away issuers' ability to evaluate them. Other merchants populate the fields with irrelevant or static information, leading to declines due to mismatches.

If conditional or optional fields are not provided, then they should be empty and not space filled (which will be rejected by the Directory Server).

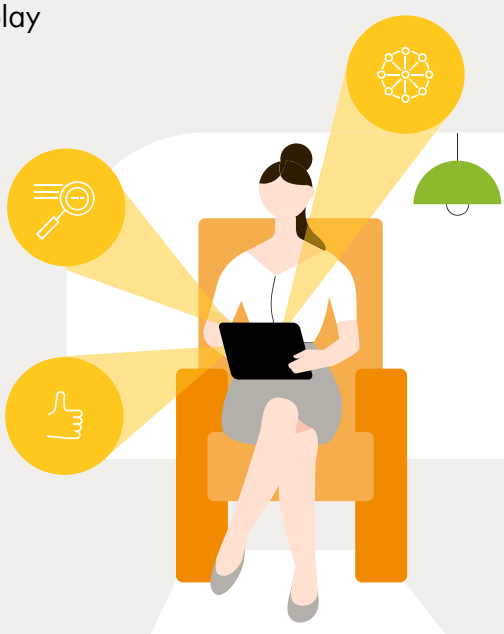
The Merchant Category Code (MCC) is important for risk assessment, and should be accurately populated to reflect the merchant's business – ideally the same as in the authorisation.

4. Using error messages with EMV 3DS

When issuer declines authentication request or challenge fails, issuer/ACS should provide, and merchant should display potential error messages / cardholder communication:

- Cardholder Info in AReq
- Challenge Info Text in Cres

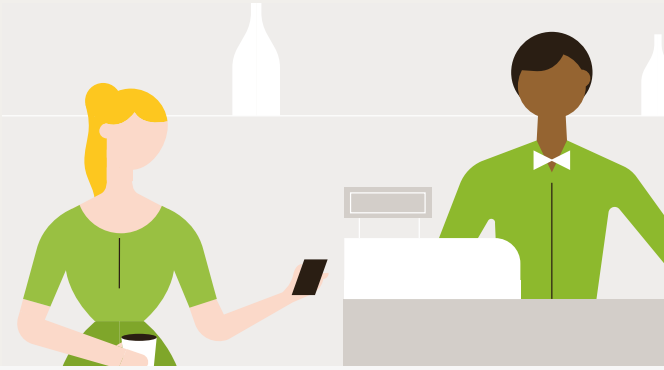
This will allow cardholder to act (e.g. enroll, unblock card, etc. by contacting issuer) and retry authentication.



5. Do not send rejected authentications to authorisation

The merchant must not retry with 3DS 1.0 or send the transaction to authorisation if an EMV 3DS authentication request fails with Transaction Status “R” (Authentication / Account Verification Rejected; Issuer is rejecting authentication / verification and request that authorization not be attempted) or CRes = “N”.

In case of transaction declined or cancelled by the cardholder, the transaction cannot be sent to authorisation. This will avoid declined or cancelled authentications billed to cardholders.



6. Soft decline processing

If issuers require SCA because authorisation was not preceded by an authentication, then the:

1. issuer should decline the authorisation with reason code 65/soft decline SCA is required (in DE 39)
2. merchant should retry with EMV 3DS and Challenge Indicator 04/SCA mandated or 3DS1 if EMV 3DS is not supported by merchant or issuer
3. if authentication successful, merchant should send another authorisation with 3DS data
4. issuer should not automatically decline this fully authenticated authorisation.

If merchant cannot handle soft decline and retry with an authentication request, then each transaction should be authenticated (especially low value payment acquirer exemptions which must be challenged if counters are exceeded as per PSD2).

If the authentication (e.g. for €70) is followed by an authorisation (e.g. €100) with a higher amount, then issuers should decline with reason code 13/invalid amount, not reason code 65/soft.

7. Amount tolerance

The European Banking Authority (EBA) set out the following principles for transactions for which the final amount is unknown:

1. **The final transaction amount cannot be higher than the authenticated amount.** According to the EBA, "if the final amount is higher than the amount the payer was made aware of and agreed to when initiating the transaction, the payer's PSP shall apply SCA to the final amount of the transaction or decline the transaction".

2. **The final transaction amount may be lower than the authenticated amount.** According to the EBA, "[i]f the final amount is equal to or lower than the amount agreed in accordance with Article 75(1) of PSD2, the transaction can be executed and there is no need to re-apply SCA, as the authentication code would still be valid in accordance with Article 5(3)(a) of the [RTS]".

There are three options when the authorisation amount is higher than the authentication amount, compliant with PSD2:

1. Use of Merchant Initiated Transaction (MIT) for the payment amount (MIT is excluded from PSD2 but requires SCA when setting up with cardholder, liability with merchant)

2. **A:** Regular payment for expected amount (SCA required for expected amount with liability with issuer unless acquirer exemption applies), if needed, followed by;

   B: 2nd payment for incremental amount (no SCA either with exemption or MIT, if applicable, and liability with merchant if acquirer exemption or MIT applies)

3. Regular SCA for expected amount plus margin similar to preauthorisation value being used at hotel check in (cardholder could be informed that SCA does not block the total amount).

The 20% tolerance will be kept in the Mastercard documentation for the UK and zero amount tolerance (authorisation amounts can always be lower than authentication amounts) will be applicable to all EEA countries.