Mastercard® Identity Check™/ EMV 3-D Secure FAQs and top actions for Merchants

Reduce fraud and false declines of card-not-present transactions – with an enhanced check-out experience for cardholders

mastercard

March 2019

PSD2 RTS: what is it?

PSD2 RTS stands for the EU **P**ayment **S**ervices **D**irective **2** **R**egulatory **T**echnical **S**tandards that were published in early 2018.

PSD2 RTS require that from the 14th September 2019, Strong Customer Authentication (SCA) must be used for all remote electronic transactions, including e-commerce, unless an exemption applies (please see below for details). Merchants must therefore send authentication requests using the EMV3-D Secure (EMV 3DS) protocol to avoid that issuers decline e-commerce transactions. In recent surveys around 20% of large issuers have indicated that post-RTS, non-EMV 3DS transactions will be declined to avoid non-compliance.

The RTS aims to reduce fraud by mandating SCA for electronic payments, including card payments from browsers or in-app payments, on all types of devices. It details the requirements of when to apply SCA as well as the exemptions from SCA.

The RTS will apply in the 31 countries which make the European Economic Area or EEA (which includes the 28 EU countries plus Norway, Iceland and Liechtenstein).

EMV 3DS: what is it?

EMV 3DS is the evolution of the current authentication interface (3DS 1.0) into an industry standard that:

- Lets more transaction and consumer data be exchanged (e.g. device data, shipping and billing address), allowing the issuer to apply SCA exemptions and enhance decisioning.
- Supports new payment needs, such as in-app and mobile payments.
- Supports additional use cases, such as:
  - Credential-on-file (COF): no need for customers to enter card details into merchant/ retailer's website or app for each purchase as card is pre-registered.
  - Wallets, e.g. Google, Samsung Wallets.
  - Tokenisation: a token replaces the real card number being stored, avoiding compromise when hacked.

mastercard

Mastercard® Identity Check™: the new Mastercard programme supporting merchants and the RTS

Mastercard Identity Check is the new programme and brand for Mastercard authentications based on the EMV 3DS standard. It replaces the former SecureCode® programme (which could ultimately still serve as fallback) and the previous EMV 3DS version as of April-December 2019 (depending on the country).

Identity Check requires minimum performance levels for authorisation approvals, fraud and abandonments to be met by issuers.

European issuers will also be required as of April 2019 (September 2019 in some countries) to offer their cardholders biometric authentication solutions via smart phones, which have the lowest abandonment and fraud rates, therefore resulting in the highest sales conversion rates.

EMV 3DS and Identity Check: an opportunity for merchants

With EMV 3DS and Identity Check, e-commerce merchants will be able to achieve the same performance levels as physical store merchants (using Chip & PIN, as measured on the Mastercard network*):

- on average 10 percentage points higher approval rates
- up to 50% reduced fraud rates
- around 50% lower abandonment rates

These results can be achieved by letting issuers apply SCA to every online purchase and providing them with sufficient data to apply exemptions from SCA, so transactions can be completed with minimal friction. Online merchants must support EMV 3DS authentication requests to comply with PSD2 RTS and Mastercard rules as of April-December 2019 (depending on country).

*Mastercard transaction data 2017

mastercard

SCA exemptions: when and how are these applied?

The RTS allows Payment Service Providers (e.g. issuers and acquirers) to apply the following exemptions for remote transactions:

- For low value payment transactions equal to or below €30; however even low value payments require SCA for every sixth transaction, or if the cumulative amount is higher than €100 since the last SCA.
- For recurring payment transactions of the same amount and payee. SCA is required when setting up the initial recurring payment agreement including a correct setting of the amount, expiration and frequency of the recurrence. Subsequent recurring transactions shall include reference to the initial agreement.
- When applying transaction risk analysis (TRA) of payment transactions for which the amount and fraud level do not exceed pre-defined limits as per the RTS (e.g. a payment initiated by a cardholder that has not generated any fraud scenarios before, from the same device as used during previous purchase, for an amount up to €100 and where the acquirer fraud levels do not exceed 13 basis points).
- For transactions to merchants that were listed by cardholders as trusted beneficiaries (so-called 'white-list' exemption). SCA is required for the creation or amendment of the white-list of trusted beneficiaries. Only issuers may apply this exemption. Unless the acquirer applies an SCA exemption, the issuer is liable for fraud if an authorization was approved, provided that the merchant sent an authentication request for the transaction.

Authentications using EMV 3DS are the recommended method for the merchant to advise the issuer about the exemption being applied by the acquirer. Such authentications typically won't require a cardholder challenge (e.g. could not lead to an abandonment) but they will allow the issuer to control the risk which increases the approval rate.

To comply with PSD2 RTS, as of 14 September 2019 merchants must use 3DS authentication requests unless an acquirer exemption applies. Authorization without authentication is allowed if an acquirer exemption is applied as per PSD2 RTS, however, such transactions usually have lower approval rates.

What are the top actions merchants need to take?

1. Merchants must select and deploy their PSP (Payment Service Provider/3DS Server) that implements and operates the authentication interface on their behalf through EMV 3DS and 3DS 1.0 (as fallback when issuer does not support EMV 3DS).
2. Merchants must prepare themselves to capture incremental transaction and cardholder data (e.g. billing and shipping address, e-mail, mobile phone number or device ID) and send them to the PSP which may require the coding for a new API (Application Programming Interface) or similar provided by the PSP. Merchants shall ensure that their terms and conditions reflect the collection and sharing of the consumer data (e.g. in the privacy notice) as required for example by the General Data Protection Regulation (GDPR).
3. Merchants need to implement an authentication policy, aligned with their PSP and acquirer, in support of the RTS and its exemptions, specifically to the adoption of TRA exemptions and corresponding fraud levels that apply.

4. Merchants must ask their acquirer(s) to enrol them for EMV 3DS with the card schemes.
5. Merchants need to make changes to their websites in support of EMV 3DS, the RTS and Mastercard Identity Check. One of these changes is the adoption of the Mastercard Identity Check programme logo.
6. Should a merchant request an acquirer SCA exemption without an authentication request, and the transaction is declined by the issuer (especially for reasons other than financial or technical declines), then a mechanism should be in place that automatically sends an EMV 3DS authentication requesting a challenge and, if approved, followed with another authorisation. Similarly, if an issuer does not yet support EMV 3DS authentications then a merchant should use the current 3DS version 1.0.2 as a fall back.
7. Merchants must ensure name consistency and uniqueness. Best performance of authentication and authorization processes is obtained when merchant name is consistent. Merchants may benefit optimally from white-list exemptions when they can be recognized with one unique name.
8. Merchants are recommended to always send authentication requests, especially with Issuers that decline authorizations without prior authentication.
9. Integrate EMV 3DS features to offer an optimal end-consumer experience, by revamping the authentication part of the merchant app in native User Interface (UI) to offer the same look and feel as the merchant app.
10. Merchants have to apply SCA to the first recurring payment. In order to increase the approval rates, it is recommended that for each subsequent payment an EMV 3DS authentication request is sent to the issuer with a reference to the initial SCA to avoid that the cardholder is asked to authenticate.
11. In case of recurring payments for variable amounts or payments where the final amount is not known, the Merchant should clearly communicate and explain to the end consumer the reasons why the authenticated amount could be different than the final authorization amount. Additional amounts should anyway be within reasonable customer expectations.

For further information please contact your Mastercard Representative.

mastercard