AN 2723 Revised Standards for Europe Region PSD2 RTS Compliance for Remote Electronic Transactions

Type:
Bulletin Announcement

Category:
Operations
Rules/Standards
Security

Audience:
Acquirer
Issuer
Processor
Engage Partner

Country:
European Economic Area
United Kingdom
Gibraltar

Brand:
Mastercard®
Debit Mastercard®
Maestro®

Action Indicator:
Network Mandate
Program or service requirement
Critical action needed

System:
Account Level Management
Authorization
Clearing

Published:
9 March 2021

Effective:
1 July 2019
14 September 2019
18 October 2019
1 February 2020
1 July 2020
1 January 2021

Executive Overview

Mastercard is updating various details regarding core information previously published.

Mastercard previously announced revised Standards to facilitate issuer and acquirer compliance with the Payment Services Directive 2 (PSD2) Regulatory Technical Standards (RTS). Mastercard also previously introduced a series of mandates, rules, and date changes as well as documentation to facilitate compliance of all ecosystem parties with the PSD2 RTS in the European Economic Area (EEA) countries.

This bulletin announcement contains the scheme-related rule changes in the *Mastercard Rules* and the *Transaction Processing Rules* manuals. Changes to the specific rules for the Mastercard switch were published separately.

This bulletin announcement does not cover Standards, requirements, nor guidelines for the adoption of PSD2 RTS compliance on use cases performed on digital wallets.

Failure to comply with any of the rules described in this bulletin announcement may result in an assessment as of 1 January 2021 (1 October 2021 in United Kingdom) of EUR 25,000 per type of non-performance.

Effective Date Details

Date	Details
1 January 2021	• Acquirers are responsible for updating contractual agreements with merchants to confirm the appropriate application of secure corporate tool flags and merchant-initiated transaction (MIT) agreements. • Issuers are responsible for updating contractual agreements with corporate customers to confirm that corporate travel tools are secure. • Acquirers must properly flag "no proof of authentication" MIT authorization message.

Date	Details
1 January 2021 (continued)	• Issuers must not challenge more than five percent of all authentication requests carrying an acquirer exemption flag or strong customer authentication (SCA) delegation flag. Failure to comply with any of the rules described in this bulletin announcement may result in an assessment as of 1 January 2021 (1 October 2021 in United Kingdom) of EUR 25,000 per type of non-performance.
14 September 2020	• Soft Decline to Request SCA Mandate • Recurring Payments Transactions Mandate • MIT Mandate • Mandate to Set Merchant Transaction Risk Analysis (TRA) Flag in ISSM • Trace ID Mandate
1 July 2020	• Exemption/Exclusion Indicator Mandate • Country Code Mandate
18 October 2019	Liability Shift for EMV[1] 3D-Secure (3DS) Merchant Attempts
14 September 2019	Amount Recommendation
1 July 2019 1 April 2020 1 July 2020 14 September 2020	Merchant Name Mandates

Customer Benefit

For ease of reference, this bulletin announcement makes reference to the Mastercard switch-specific requirements. If an alternate switch is used for processing transactions, then the corresponding requirements of that switch would replace those for the Mastercard switch.

What Mastercard is Doing

Mastercard has published an *Authentication Guide for Europe* on Mastercard Connect™ that provides all parties with more details and background about the changes.

Due to the complexity of the business models and the significant number of parties involved in the processing of transactions, the Travel & Hospitality sector requires specific measures to achieve regulation compliance, short and long term.

[1] EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries.

Version History

Date	Description of Change
9 March 2021	• Included details in the Amount Recommendation section regarding soft declines. • Included Digital Secure Remote Payment (DSRP) details in the Exemption/ Exclusion Indicator Mandate section. • Added details regarding the 14 September 2020 effective date in the Soft Decline to Request SCA Mandate section. • Added details regarding PSD2 RTS article 17, as well as Secure Corporate Payment exemptions, in the Secure Corporate Payments (SCP) section. • Updated the terminology throughout from noncompliance penalties to assessments. • Added a new Related Information section. • Added a new Merchant Initiated Pre-Authorizations section.
24 August 2020	• Added mandates and rules to address Travel & Hospitality industry requirements related to third party indirect sales and secure corporate payments. • Added a recommendation to retry with a 3DS v1 (3DS1) authentication or a non-3DS authorization when issuers decline authorizations authenticated through EMV 3DS. • Clarified the values of key fields in an initial and subsequent recurring and MIT payment. • Clarified the use of Trace ID in other than card-not-present (CNP) environments.
11 November 2019	• Revised the effective dates of the various mandates and rules to align with the revised European Banking Authority (EBA) Opinion and Guidelines and the migration plans as approved by local competent authorities. • Added a new value 06 = Secure Corporate Payment as an exemption/exclusion indicator. • Added that acquirers must ensure, as of 1 April 2020, the merchant name used during authentication and registered in the Identity Solutions Services Management (ISSM) tool is not used by another merchant. • Removed the requirement to provide the merchant country code in ISSM. • Added that, as of 14 September 2020, setting up an MIT requires an authorization request (either an authorization request or account status inquiry). • Added that for CNP authorizations, Response Code 65 cannot be used for other reasons than requesting SCA. • Added a recommendation to try again with a 3DS1 authentication or a non-3DS authorization if issuers decline authorizations with EMV 3DS (attempted or fully authenticated).
31 May 2019	Initial publication date

EBA Opinion on Soft Enforcement

The EBA issued an opinion on 21 June 2019 allowing National Competent Authorities (NCAs) to agree on a migration plan to accomplish a soft enforcement of the PSD2 RTS regulation. On 16 October 2019, the EBA issued an opinion on the soft enforcement transition period to have a maximum duration of 15 months (starting the hard enforcement on 1 January 2021).

NCAs across the Europe region are building migration plans, with most of these plans in line with the EBA recommendation for limited duration.

Different PSD2 RTS Effective Date in UK of Brexit

On 30 April 2020 the Financial Conduct Authority (FCA – the NCA for the UK) has updated its position providing the industry an additional 6 months to implement SCA for e-commerce. The new timeline of 14 September 2021 replaces the previous 14 March date. A revised implementation plan is being developed.

For customers in UK and EEA these date differences of the Brexit agreement may impact the CNP transactions that have one leg in UK and the other leg in EEA respecting the EBA opinion that SCA applies between markets where such proper SCA infrastructure is in place:

- EEA issuers can accept non-SCA transactions from UK acquirers and vice versa, UK issuers can accept non-SCA transactions from EEA acquirers until 14 September 2021
- As of the 14 September 2021, EEA issuers must apply SCA also for transactions initiated by UK acquirers and vice versa, UK issuers must apply SCA for transactions from EEA acquirers

The above statements hold as long as the FCA continues to apply the same PSD2 principle of application of SCA to one-leg transactions.

PSD2 RTS Compliance

The following sections provide PSD2 RTS compliance details.

Reminder Identity Check/EMV 3DS Liability

The existing fraud chargeback protection for e-commerce merchants that use Mastercard® SecureCode™ will also apply for transactions using Identity Check/EMV® 3DS authentications in the EEA.

It is already effective when the issuer approves an EMV 3DS authentication. The effective date for this liability shift for 3DS merchant attempts was 18 October 2019.

Amount Recommendation

As PSD2 RTS principle, the authentication amount for a Remote Electronic Transaction must be an amount that the cardholder would reasonably expect and the authentication must use the same currency as the authorization.

Whereas the UK FCA takes a position that the total transaction amount of all authorizations that relate to a remote electronic transaction should not exceed the authentication amount for the transaction by more than 20 percent, the recent EBA Q&A on Dynamic Linking has clarified that for intra-EEA transactions (except United Kingdom) the authorization amount (or the sum of these) cannot be higher than the authentication amount. Authorization amounts can be lower than authentication.

Merchants that operate in business models where the final amount is not known at the time of authentication may have several options allowing them to remain regulation compliant:

1. By adding a margin to the authentication amount accompanied with clear consumer information and education about the ultimate impact on funds blocking (similar to the processes used at hotel check-in) with benefit of liability shift.

2. By setting up a Merchant Initiated Transaction (MIT) agreement for a zero amount (requires SCA at set-up and requires clear consumer communication of the MIT T&Cs including the potential maximum amount to be debited before and after authentication). Subsequent MIT(s) can be initiated for the final (maximum) amount as these are out-of-regulation-scope but carry merchant liability.
3. By setting up a Merchant Initiated Transaction (MIT) agreement for the known amount followed by an authorization for the same amount with benefit of liability shift. Subsequent MIT(s) can be initiated for the remaining (up to maximum) amount as these are out-of-regulation-scope but carry merchant liability.

If the authentication is followed by an authorization with a higher amount, then issuers should decline with reason code 13 (Invalid Amount), not reason code 65 (Soft Decline SCA is Required). This will inform the merchant to perform another authentication with the correct amount or split the transaction in two. Issuers should not apply soft decline for other reasons than when SCA is required.

If the transaction amount exceeds the cardholder's "reasonable expectations, or if the final transaction amount is higher than stipulated in the MIT agreement," the refund right for authorized transactions under Articles 76-77 PSD2 may apply. This rule does not apply to recurring payment transactions.

Exemption/Exclusion Indicator Mandate

As of 14 September 2020, in the Authorization Request/0100 message for an intra-EEA Remote Electronic Transaction that is subject to PSD2 RTS, authentication can only be skipped if an acquirer exemption to Strong Cardholder Authentication (SCA) applies or if an exclusion to SCA applies or:

- When the transaction is originating from a secure corporate payment platform that allows the issuer to apply an SCA exemption due to "secure corporate payment processes or protocols" or
- If another SCA-compliant method was used (such as delegation to the merchant, Secure Corporate Payment exemption applied with the merchant's knowledge).

When SCA by the issuer may not be required under PSD2 RTS (or when it has been delegated through Authentication Express Type 2 or when the transaction originates from a secure corporate payment platform that allows the issuer to apply an SCA exemption due to secure corporate payment processes or protocols), the acquirer must provide the reason by populating the appropriate value in Data Element (DE) 48, subelement 22, subfield 1 in the authorization message:

- 01 = Merchant Initiated Transaction
- 02 = Acquirer low fraud and Transaction Risk Analysis
- 03 = Recurring payment
- 04 = Low value payment
- 05 = SCA Delegation under Authentication Express Type 2
- 06 = Secure Corporate Payment (for more information, refer to AN 2645 Enhancement to Low-Risk Transaction Indicator)
- 07 = Authentication Outage Exception (for more information, refer to AN 4040 New Value in Low-Risk Transaction Indicator Field)

DSRP transactions will not carry an SCA delegation flag in DE 48, subelement 22, subfield 1.

Effective 1 July 2020, an issuer must be able to process DE 48, subelement 22, subfield 1 in the authorization message as part of PSD2 RTS exemption and exclusion regulation.

Issuers must not systematically decline (including soft declines with Response Code 65) authorizations with DE 48, subelement 22, subfield 1, even if non-3DS. Issuers must not step-up more than 5 percent of all authentications with acquirer exemption, exclusion, or delegation flag (in the EMV 3DS version 2.1 Merchant Data Field 1 [SCA Exemptions] and as of EMV 3DS v2.2 Challenge Indicator, value of 05 or 07).

As of 14 September 2020, acquirers in the EEA that allow their online merchants to request a Transaction Risk Analysis (TRA) exemption under PSD2 RTS must set the TRA exemption flag for such merchants when

registering them for the Identity Check Program in the Identity Solutions Services Management (ISSM) tool. Mastercard may monitor compliance in the future by verifying if the merchant name used in the authorization message has the right to use the acquirer TRA exemption as specified in the ISSM tool (based on the merchant name registered for authentications).

In order to optimize authorization approval rates for transactions using an acquirer exemption under PSD2 RTS, it is recommended that merchants send an EMV 3DS authentication request with the acquirer exemption flag.

EEA acquirers and issuers must ensure, as of 1 July 2020, that the "acquirer exemption" flag (used for all acquirer exemptions, such as low value payment and TRA exemption and recurring payment) is supported in EMV 3DS authentication requests.

This must be flagged in EMV 3DS version 2.1 Merchant Data Field 1 (SCA Exemption) with value 05/No SCA Requested, Transaction Risk Analysis performed and as of EMV 3DS v2.2 Challenge Indicator value 05/No SCA Requested, Transaction Risk Analysis performed.

Mastercard recommends that acquirers send the acquirer exemptions through EMV 3DS, and not through authorization only. In case the acquirer's transaction model needs to avoid a challenge from the issuer (such as a recurring payments, MIT, and certain cases of low value payments), then the acquirer can send an Identity Check Insights (formerly referred to as data-only) EMV 3DS message. This will ensure a higher approval ratio, as the issuer will receive the digital transaction insights from Mastercard and will be able to assess the risk more accurately. For more details, refer to AN 1803 Acquirer Exemptions for Strong Customer Authentication under PSD2 and the RTS.

EEA acquirers with online merchants accepting corporate cards, as well as corporate card issuers, must ensure, as of 1 July 2020, that the EMV 3DS version 2.1 Merchant Data Field 4 (Secure Corporate Payment) (which indicates if the conditions for the Secure Corporate Payment exemption are met and hence if the exemption can be applied by issuers) can be supported. The details of these EMV version 2.1 Merchant Data fields were announced in AN 2758 Announcing the New EMV 3DS 2.1 Mastercard Message Extension in EEA Countries.

Merchant Name Mandate

The following additional rule applies to intra-EEA Transactions. As of 1 July 2020, acquirers must ensure that their online merchants always use the same merchant name in the authentication message. The merchant name in authentications must uniquely identify the merchant in all countries where it operates and for all its activities (for example, Merchant.com) or per its activities (such as MerchantBooks.com, MerchantMusic.com) or per its countries (such as Merchant.fr, Merchant.co.uk). Acquirers must ensure that the merchant name used by the merchant actually belongs to the merchant and is registered for using the Identity Check Program.

It is recommended that acquirers use the same merchant name in authentication and authorization as this facilitates dynamic linking under PSD2 RTS and compliance monitoring of merchant's acquirer's usage of the acquirer TRA exemption. For payment facilitators, the merchant name used in authentication is recommended to mirror the one in authorizations, such as "Payment Facilitator * Submerchant".

As of 1 July 2019, acquirers in the EEA must register the merchant name used in EMV 3DS authentication messages in the Identity Solutions Services Management (ISSM) tool. Submerchants behind Payment Facilitators do not need to be registered if the Payment Facilitator is registered in ISSM (in the format "Payment Facilitator *"), but this means that ISSM flags and fields for services like merchant white listing, Authentication Express, and acquirer TRA exemptions will not work at the sub-merchant level. As of 1 February 2020, acquirers in the EEA must register the country code for merchants using EMV 3DS authentication messages in the Identity Solutions Services Management (ISSM) tool.

Acquirer Country Code Mandate

As of 14 September 2019, if the issuer and the acquirer are in the EEA but the merchant is not, EMV 3DS authentication requests must include the EMV 3DS version 2.1 Merchant Data with Field 3 (acquirer country

code) containing the acquirer country code. In other cases, it is recommended to provide the acquirer country in the EMV 3DS version 2.1 Merchant Data Field 3.

The issuer and its Access Control Server are recommended to use the acquirer country code in the EMV 3DS version 2.1 Merchant Data Field 3 to determine if SCA is required by PSD2 RTS. If the acquirer country code is not provided, then issuers are recommended to use the merchant country to determine if SCA is required by PSD2 RTS.

Recurring Payments Transactions Mandate

As of 14 September 2020 for intra-EEA recurring payment transactions, acquirers must provide the unique Trace ID of the initial recurring payment authorization in DE 48, subelement 63 (Trace ID) of subsequent recurring payment transaction authorizations to allow the issuer to validate that SCA occurred on the initial recurring payment authorization, as is required under PSD2 RTS.

This rule applies to recurring payments initiated in a card-not-present environment such as e-commerce and mail order/telephone order as well as in a card-present (face-to-face) environment.

This rule does not apply to reversals, which must continue to include the Trace ID of the authorization to be reversed. Refer to release announcement AN 2630 Use of Trace ID to Support PSD2 Recurring Payment Requirements for more details.

If the initial authorization happened before 14 September 2020, or if the recurring payment was set-up as a MO/TO, or in a card-present (face-to-face) environment with the initial Trace ID not available (for example, was not stored), then the Trace ID must have the following "dummy" values:

- Positions 1-3 = MCC
- Positions 4-9 = 999999
- Positions 10-13 = 1231
- Positions 14-15 = blank filled

Alternatively, if the initial authorization occurred before 14 September 2020, then the Trace ID can refer to any other authorization belonging to that same recurring payment arrangement provided this authorization took place before 14 September 2020.

Effective 1 July 2020, the issuer is recommended to be able to store the Trace ID so that it is able to validate that SCA took place when setting up the recurring payment arrangement. This Trace ID will be considered as the reference to the mandate that the cardholder provided to and authenticated with the merchant.

As of 14 September 2020, EEA issuers must be able to process the Trace ID provided in authorizations in DE 48, subelement 63 (Trace ID), for example to validate if an initial SCA occurred to set-up the recurring payment arrangement as required under PSD2 RTS.

Effective 14 September 2020, for remote electronic transactions effected in the EEA, the transactions in a series of recurring payment transactions will require:

- the initial authorization
  - to be flagged as recurring payment through DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 4 (Standing order/recurring transactions)
  - to be flagged as a fully authenticated and challenged transaction through DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator), value 212 or 217 and through DE 48, subfield 43 (UCAF Authentication Value) value with leading indicator kB or kP
  - not to be flagged having an exemption; ie DE 48, subelement 22 (Multi-Purpose Merchant Indicator), subfield 1 (Low-Risk Merchant Indicator) should not be populated
  - not to carry an original Trace ID through DE 48, subfield 63 (Trace ID)
- the subsequent authorization(s)

- to be flagged as recurring payment through DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence) value 4 (Standing order/recurring transactions)
- to be flagged having an exemption through DE 48, subelement 22 (Multi-Purpose Merchant Indicator), subfield 1 (Low-Risk Merchant Indicator) value 03 (Recurring Payment Exemption) unless DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator) has a value 211, 212 or 217 in which case the transaction is not to be flagged having an exemption
- to carry an original Trace ID through DE 48, subfield 63 (Trace ID) from the initial authorization unless DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator) has a value 211, 212 or 217 in which case the transaction is not to carry an original Trace ID but rather an Authentication Value in DE 48, subelement 43 (3-D Secure for Mastercard Identity Check)

Issuers should not decline the initial authorization when it contains non-relevant data such as DE 48, subelement 22 (Multi-Purpose Merchant Indicator), subfield 1 (Low-Risk Merchant Indicator) and/or DE 48, subfield 63 (Trace ID).

Merchant-Initiated Transactions Mandate

Acquirers subject to PSD2 RTS are only allowed to apply Merchant Initiated Transactions (authorization requests with an MIT exemption indicator) when:

- The transaction is triggered by the merchant when the cardholder is off-session (off-session means the cardholder is not interacting with the merchant page or the merchant app to initiate the transaction), or
- The transaction is triggered by the merchant as it could not have been triggered by the cardholder during checkout, because:
  - The final amount is not known during the checkout (for example, online groceries shopping), or
  - An event triggered the transaction after the checkout (for example, miscellaneous rental or service charges), or
  - The transaction is part of a recurring payment arrangement, or
  - The transaction is broken down into different payments happening at different times (for example, installments, travel bookings, market places), or
  - The transaction is a staged-wallet funding transaction where the funding is triggered without the involvement of the cardholder (e.g. "top-up" scenario), or
  - The transaction follows upon a declined authorization at a transit validator but the traveler has completed a billable journey (Transit Debt Recovery)

As of 14 September 2020, to set-up each individual MIT, SCA is required, as well as an agreement between the merchant and the cardholder specifying the reason for the payment and the payment amount (or an estimate when the precise amount is not known).

The MIT exclusion cannot be used to bypass the PSD2 SCA requirements for transactions for which card data has been registered on file with the merchant and the cardholder triggers the payment (Card-on- File).

MIT must be flagged by populating DE 48, subelement 22, subfield 1 in the authorization message with 01 = Merchant Initiated Transaction. Refer to release announcement AN 2609 Enhancements to Low- Risk Transaction Indicator to Support EEA Customers Compliance to PSD2 RTS for more details.

As of 14 September 2020, setting-up an MIT requires an authorization request (either an authorization request or account status inquiry) in order to allow the issuer to validate the authentication value generated for the agreement.

An acquirer must use an account status inquiry when the MIT agreement has been established for a zero amount.

As of 14 September 2020 for intra-EEA MITs, acquirers must provide the unique Trace ID of the initial MIT authorization in DE 48, subelement 63 (Trace ID) of subsequent MIT payment transaction authorizations to allow the issuer to validate that SCA occurred on the initial MIT authorization, as is required under PSD2 RTS.

This rule applies to MIT agreements initiated in a card-not-present environment such as e-commerce and MO/TO as well as in a card-present (face-to-face) environment.

This rule does not apply to reversals, which must continue to include the Trace ID of the authorization to be reversed. Refer to the release announcement AN 2630 Use of Trace ID to Support PSD2 Recurring Payment Requirements for more details.

If the initial authorization occurred before 14 September 2020, and the initial Trace ID is not available (for example, was not stored), or if the MIT was set-up via mail order, telephone order, or via face to face and the initial Trace ID is not available, then the Trace ID must have the following values:

- Positions 1–3 = MCC
- Positions 4–9 = 999999
- Positions 10–13 = 1231
- Positions 14–15 = blank filled

Alternatively, if the initial authorization occurred before 14 September 2020, then the Trace ID can refer to any other authorization belonging to that same MIT arrangement provided this authorization took place before 14 September 2020.

Effective 1 July 2020, the issuer is recommended to be able to store the Trace ID so that it is able to validate that SCA that took place when setting up the MIT payment arrangement. This Trace ID will be considered as the reference to the mandate that the cardholder provided to and authenticated with the merchant.

As of 14 September 2020, EEA issuers must be able to process the Trace ID provided in authorizations in DE 48, subelement 63 (Trace ID), for example to validate if an initial SCA occurred to set-up the MIT as required under PSD2 RTS.

Issuers should expect to receive and not systematically decline MIT authorization requests for MIT agreements that have either been set up in a card-not-present environment such as e-commerce and MO/TO as well as in a card-present (face-to-face) environment, or that either have an original or dummy Trace ID.

Effective 14 September 2020, for remote electronic transactions effected in the EEA, MITs will require:

- the initial authorization
  - to be flagged as recurring payment through DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 4 (Standing order/recurring transactions), even if it is a non-recurring payment; this allows the issuer to store the Trace ID to be able to validate that SCA was used during subsequent MIT authorizations
  - to be flagged as a fully authenticated and challenged transaction through DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator) value 212 or 217 and through DE 48, subfield 43 (UCAF Authentication Value) value with leading indicator kB or kP
  - not to be flagged having an exemption; ie DE 48, subelement 22 (Multi-Purpose Merchant Indicator), subfield 1 (Low-Risk Merchant Indicator) should not be populated
  - not to carry an original Trace ID through DE 48, subfield 63 (Trace ID)
- the subsequent authorization
  - to be flagged as recurring payment through DE 61 (Point-of-Service [POS] Data), subfield 4 (POS Cardholder Presence), value 4 (Standing order/recurring transactions)
  - to be flagged having an exemption through DE 48, subelement 22 (Multi-Purpose Merchant Indicator), subfield 1 (Low-Risk Merchant Indicator), value 01 (Merchant Initiated Transaction) unless DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level

Indicator) has a value 211, 212 or 217 in which case the transaction is not to be flagged having an exemption
  - to carry an original Trace ID through DE 48, subfield 63 (Trace ID) from the initial authorization unless DE 48, subelement 42 (Electronic Commerce Indicators), subfield 1 (Electronic Commerce Security Level Indicator) has a value 211 , 212 or 217 in which case the transaction is not to carry an original Trace ID but rather an Authentication Value in DE 48, subelement 43 (3-D Secure for Mastercard Identity Check)

Issuers should not decline the initial authorization when it contains non-relevant data such as DE 48, subelement 22 (Multi-Purpose Merchant Indicator), subfield 1 (Low-Risk Merchant Indicator) and/or DE 48, subfield 63 (Trace ID).

Merchant Initiated Pre-Authorizations

Referring to an initial transaction through the original Trace ID is a common theme for subsequent MITs as well as to identify an incremental amount pre-authorization and zero amount Authorization Chargeback Protection Period Extension request.

In exceptional circumstances, the original Trace ID in DE 48, subelement 63 of the authorization request can refer to both the initial authorization confirming the MIT agreement as well as the original pre-authorization request. This use case could surface when a pre-authorization was initiated in the context of an MIT agreement and where part of the shipment was not delivered within the standard chargeback protection period. In such case, a pre-authorization extension of the chargeback protection period is required and must be flagged as an MIT exemption (DE 48, subelement 22, subfield 1, value 01) and both DE 61, subelement 4 and DE 61, subelement 7 would be populated with a value of 4.

The combination of a subsequent MIT payment and pre-authorization is only allowed for incremental preauthorizations for a zero amount to extend the chargeback protection period associated with the original preauthorization.

An incremental pre-authorization cannot be combined with a subsequent recurring payment (DE 48, subelement 22, subfield 1, value 03) nor can an incremental pre-authorization for an additional amount be combined with a subsequent MIT payment.

Soft Decline to Request SCA Mandate

The Regulatory Technical Standards (RTS) defined for PSD2 also require SCA for CNP transactions unless an exemption applies. Therefore, issuers must inform merchants when SCA is required.

As of 14 September 2020:

- Issuers in the Europe region that receive an authorization without prior authentication and decide they must require SCA (as of when PSD2 RTS or market approved migration plans requires them to or in case of suspicion of fraud) must only decline the authorization with Response Code 65 (in DE 39). For CNP authorizations, this Response Code 65 cannot be used for other reasons than requesting SCA. It cannot be used if a 3DS approved authentication preceded the authorization which is flagged as fully authenticated (Service Level Indicator 212 in DE 48, subelement 42).
- Furthermore, Response Code 65 should not be used for transactions that are fully authenticated by merchants or wallets and are in compliance with the PSD2 regulation, including:
  - Device-based DSRP transactions, which are fully authenticated using the consumer device cardholder verification method (CDCVM). For more information about device-based DSRP transactions, refer to the *MDES Issuer Implementation Guide*.
  - Server-based (cards on file) transactions with delegated authentication, which are fully authenticated using a merchant or wallet's SCA mechanism compliant with the Authentication Express program. For more information about server-based transactions with delegated authentication, refer to the *Authentication Express Program Guide*.

As of 1 July 2020:

- Acquirers' online merchants in the Europe region must initiate an EMV 3DS authentication with 3DS Requestor Challenge Indicator set to 04 (Challenge requested: Mandate) in response to a declined authorization message with Response Code 65. When tokenized credentials are used, the acquirer must not submit the same DSRP cryptogram in the declined authorization message and in the new authorization request. In order to maintain cardholder user experience consistency, the acquirer must not request the cardholder to re-enter card data or any other data before performing the retry of the transaction that was previously soft-declined by the issuer. Until all issuers support Response Code 65, merchants are recommended to always send an authentication request following a non-3DS authorization that was declined for non-financial and non-technical reasons.

It is recommended that Europe region acquirers' online merchants retry with a 3DS1 authentication if the EMV 3DS authentication response has Transaction Status A (Attempts) and the merchant is enrolled in 3DS1. Transaction Status A will be used by Smart Authentication Stand-In when an EMV 3DS authentication request cannot be approved or when a card is not enrolled for EMV 3DS, in which case, trying again with a 3DS1 authentication is likely to be approved, which leads to higher authorization approval rates.

Similarly, if issuers decline authorizations that have been sent for EMV 3DS authentication by the merchant (attempted or fully authenticated by Smart Authentication Stand-In RBA as indicated by the leading indicator of the AAV equal kJ, kC, kL, kE), then trying again with a 3DS1 authentication or a non-3DS authorization is recommended when the reason for declining is non-financial, non-technical or soft decline.

Travel & Hospitality (T&H) Sector Recommendation and Mandate

Two use cases specific to the T&H sector require special measures in support of regulation compliance while minimally impacting business performance:

- Indirect Sales through Third Party Agent
- Secure Corporate Payments (PSD2 RTS art. 17)

The below measures have an impact on the T&H Sector and all entities that are involved in its transaction processing. Acquirers must communicate these measures to their merchants, if necessary update contracts and T&Cs to facilitate adoption. Merchants are responsible for taking these measures to the entities they are using for transaction processing.

Indirect Sales through Third Party Agent

In an Indirect Sales model, different entities are involved in the online booking (authentication) and the subsequent payment(s) (authorization). Most often, one online booking may lead to one or more payments of varying or unknown amount and spread over an extended time period. Consequently, all subsequent payments must be considered as merchant-initiated transaction (MIT).

Due to the number of entities touching the transaction between booking and payment, data allowing merchants to initiate the payment with proof of authentication is not available to them. Mastercard has contributed to the United Kingdom Finance T&H Special Interest Group "Technical Guidance" publication defining the "proof of authentication" data elements that need to be passed along through all entities up to the merchant. Merchants must ensure they upgrade their systems to provide proof of authentication for these transactions as soon as they can. At the appropriate time, Mastercard will require that Acquirers and T&H merchants must be able to provide "proof of authentication" during subsequent authorization(s).

Based on the principle that every indirect sales transaction may lead to an MIT authorization, it is most critical towards PSD2 RTS compliance that at time of online booking the third party agent presents an MIT agreement for SCA to the cardholder. To that end:

- Merchants are responsible for putting in place or updating contractual agreements with these customer facing third party agents to confirm

  - that an MIT agreement is presented to the cardholder (refer to the *Mastercard Authentication Guide for Europe* for the recommended definition of an MIT agreement) at time of booking and before authentication that clearly defines the T&Cs of the agreement
  - the MIT agreement is confirmed through SCA as per PSD2 RTS unless a Secure Corporate Payment exemption applies as agreed by the acquirer of the merchant
- Acquirers are responsible for putting in place or updating contractual obligations with their merchants involved in indirect sales stating these aforementioned requirements.

Interim Requirements

During the time (referred to as Interim Period) where the merchant is not yet getting "proof of authentication" when initiating the MIT payment/authorization, it is expected that Acquirers flag such transactions as MIT. It is recommended, as of 1 January 2021, to use the standard identification through DE 48, subelement 22, subfield 1, value 01 (Merchant Initiated Transaction). To indicate that the merchant does not have proof of authentication, i.e. the initial Trace ID is not available, DE 48, subelement 63 must have following values:

- Positions 1–3 = MCC
- Positions 4–9 = 999998
- Positions 10–13 = 1231
- Positions 14–15 = blank filled

This default Trace ID for travel & hospitality is different from the default Trace ID used for other MIT and recurring payments using the grandfathering principle (all 9 in positions 4-9).

Refer to the Merchant-Initiated Transaction Mandate paragraph in this announcement for a complete set of MIT requirements and specifications.

Only in case the standard MIT identification cannot be implemented by 1 January 2021, the Acquirer will be allowed to keep using the DE 61, subelement 5, value 2 (mail order) or DE 61, subelement 5, value 3 (telephone order) flag until the implementation is completed, provided that SCA was performed as per PSD2. Acquirers need to take into account that lower approval rates may be experienced when applying a CNP mail order/telephone order (MO/TO) transaction identification.

Acquirers are only allowed to submit these MIT payment authorizations without proof of authentication with either the standard MIT identification or one of the existing MO/TO flags when the merchant can indicate to the acquirer that the transaction was initiated with an MIT agreement. Such indication will be assumed for bookings originating from the third party agent with whom the merchant has established a contractual agreement to support MIT agreements.

Acquirers submitting these MIT payment authorizations without proof of authentication are responsible for ensuring that no transactions are sent by them to an issuer when the transaction does not comply with the PSD2 RTS regulation. To that end:

- Acquirers are responsible for updating or putting in place contractual obligations with their merchants involved in indirect sales stating these aforementioned requirements
- Acquirers are responsible for putting in place controls to monitor these aforementioned measures

Acquirers and merchants must be aware that authorization approval rates may be influenced by the MIT indication and absence/presence of proof of authentication. T&H Sector businesses can be identified through the following MCCs:

Airlines & Air Carriers	MCCs 3000 through 3350 and 4511
Lodging	MCCs 3501 through 3999 and 7011
Car Rentals	MCCs 3351 through 3500 and 7512

Cruise Lines	MCC 4411
Travel Agencies	MCC 4722
Railways and railroads	MCC 4112 and 4011
Vacation Rental	MCC 6513
Bus Lines	MCC 4131
Ferries	MCC 4111

Issuers need to be aware that occasionally, other and non-specific T&H sector businesses can be generating such indirect sales originating MITs when being presented as part of travel packages. Package offerings are becoming increasingly popular and common practice when booking for travel. Such businesses can be identified through the following MCCs:

Taxi Cabs and Limousines	MCC 4121
Transportation Services. Not elsewhere classified	MCC 4789
Trailer Parks and Campgrounds	MCC 7033
Motor Home and Recreational Vehicle Rentals	MCC 7519
Tourist Attractions and Exhibits	MCC 7991
Aquariums, Seaquariums and Dolphinariums	MCC 7998
Insurance Sales, Underwriting and Premiums	MCC 6300
Direct Marketing. Insurance Services	MCC 5960
Government Services	MCC 9399
Parking Lots & Garages	MCC 7523
DM Insurance Services	MCC 5960

Issuers should be aware that MITs from T&H merchants that are the results of T&H bookings via third party agents are out of scope (authentication performed at mandate set up and transaction processed when cardholder no longer available) but that for an interim period, not all of these MITs will be able to bear proof of authentication due to the ecosystem upgrades required for the merchant to receive the proof of authentication.

Issuers are responsible not to systematically decline indirect sales originating MIT, either flagged with MIT indicator or through MO/TO flags, with no proof of authentication from T&H merchants or any merchant identified with one of the MCCs above.

Secure Corporate Payments (SCP)

PSD2 RTS article 17 allows issuers not to require SCA of "legal persons initiating electronic payment transactions"…"using the dedicated payment processes or protocols". Although the decision is with the competent authority of each member state, Mastercard's position is that lodged and virtual corporate and commercial cards should be exempt from SCA. Issuers manage transactions originated through lodged and virtual corporate and commercial cards in a secure payment environment, so SCP exemption could be applied without challenges. These cards can have dedicated bank identification numbers (BINs) or account ranges.

However, for physical plastic corporate cards issued to employees, typically only certain transactions are exempt. Meaning, when used at physical or online point-of-sale (POS) without dedicated processes or protocols (such as for e-commerce transactions on a public website), SCA needs to be applied. When cards are lodged with trusted suppliers using Secure Corporate Payment processes and protocols (such as, online bookings through corporate travel agents), transactions may be considered exempt under Article 17.

Secure Corporate Payment Flag

Merchants or their third party agents (such as travel management companies) that operate such dedicated payment processes or protocols can take advantage of the appropriate flags that Mastercard has defined to make the issuer aware of the secure acceptance environment and to request the issuer to apply the Secure Corporate Payment exemption:

- Data Element (DE) 48, subelement 22, subfield 1, value 06 in the authorization message
- Extension field SecureCorporatePayment = Y in EMV 3DS version 2.1 or version 2.2 authentication

Often, Merchants and/or their Third Party Agents may not know or may not have any means to identify if the card has been issued to a legal person. In order to facilitate a better performance and experience for both consumer and merchant, it is strongly recommended that merchants first authenticate the corporate purchase or booking using the SCP flag. When skipping authentication and going straight into authorization (with the SCP flag) in most instances there will be no way to return to the cardholder for authentication should the issuer not be in a position to apply the SCP exemption by soft declining the transaction. This may have a significant impact on corporate business performance.

Control Framework to Underpin SCP Flag

Based on the regulation allowing an issuer to apply the Secure Corporate Payment exemption only when the on-line booking is completed with secure and dedicated payment process and protocol, it is most critical towards PSD2 RTS compliance that at time of online booking the third party agents identify the secure environment through the SCP flag.

The following paragraphs describe a controls framework that can allow issuers to trust the indicator so the SCP exemption can be applied.

- Merchants are responsible for putting in place (or updating) contractual agreements or safeguards with these customer facing third party agents to confirm that:
  - to accept cards subject to the Secure Corporate Payment exemption a secure access must be offered to the cardholder of a "legal person" entity, a secure platform must be used to process the on-line booking and secure connections must be in place between all third party agents that are involved in the processing and switching of the transaction

    The corporate booking portal can only be used for corporate travel and by permitted users (corporate employees) and must be protected by access controls with a level of security which meets PSD2 requirements.
  - merchants that will use the exemption through a secure electronic connection (directly or indirectly via intermediaries) are connected to the corporate booking portal.
  - the SCP flag must be set and shared by the third party agent if and only if the above conditions are met, based on its knowledge that secure channel was used to make the booking.
  - authentication is obtained in case the third party agent cannot confirm that a card belongs to a legal person.
  - third party agents are responsible for putting in place or updating contractual agreements reflecting the above with other subcontracted third party agents.
- Acquirers are responsible for putting in place (or updating) contractual obligations or safeguards with their merchants to confirm these aforementioned requirements

- Acquirers submitting SCP flagged authorization and/or authentication requests are responsible for ensuring that no transactions are sent by them to an issuer when the transaction does not comply with the PSD2 RTS regulation. To that end acquirers are responsible for putting in place controls to monitor the proper use of the SCP flag.
- Acquirers and Merchants must be aware that issuers may soft decline SCP flagged authorization transactions without prior authentication request.

Based on the regulation allowing an issuer to apply the Secure Corporate Payment exemption only to cardholders that are a "legal person", it is most critical towards PSD2 RTS compliance that the issuer can properly identify those cards during authentication and authorization processing. To that end:

- "Legal Person" entities such as Corporates are responsible for putting in place (or updating) contractual agreements or safeguards with customer facing third party agents that operate the secure corporate (booking or purchasing) processes and protocols to confirm:
  - that a secure access must be offered to the cardholder of a "legal person" entity, a secure platform must be used to process the on-line booking and secure connections must be in place between all third party agents that are involved in the processing and switching of the transaction
  - whether only cards offered to a "legal person" may be accepted and if other cards may also be accepted to indicate which ones are subject to the SCP exemption
- Issuers are responsible for putting in place (or updating) contractual obligations or safeguards with their "Legal Person" entities to confirm these aforementioned requirements.

Revised Standards

To view marked revisions, refer to the attachment associated with this announcement. Additions are underlined; deletions are indicated with a strikethrough.

Related Information

- AN 2645 Enhancement to Low-Risk Transaction Indicator
- AN 4040 New Value in Low-Risk Transaction Indicator Field
- AN 1803 Acquirer Exemptions for Strong Customer Authentication under PSD2 and the RTS
- AN 2758 Announcing the New EMV 3DS 2.1 Mastercard Message Extension in EEA Countries
- AN 2630 Use of Trace ID to Support PSD2 Recurring Payment Requirements
- AN 2609 Enhancements to Low- Risk Transaction Indicator to Support EEA Customers Compliance to PSD2 RTS

Questions

Customers with questions about the information in this announcement should contact Global Customer Service using the contact information on the Technical Resource Center.