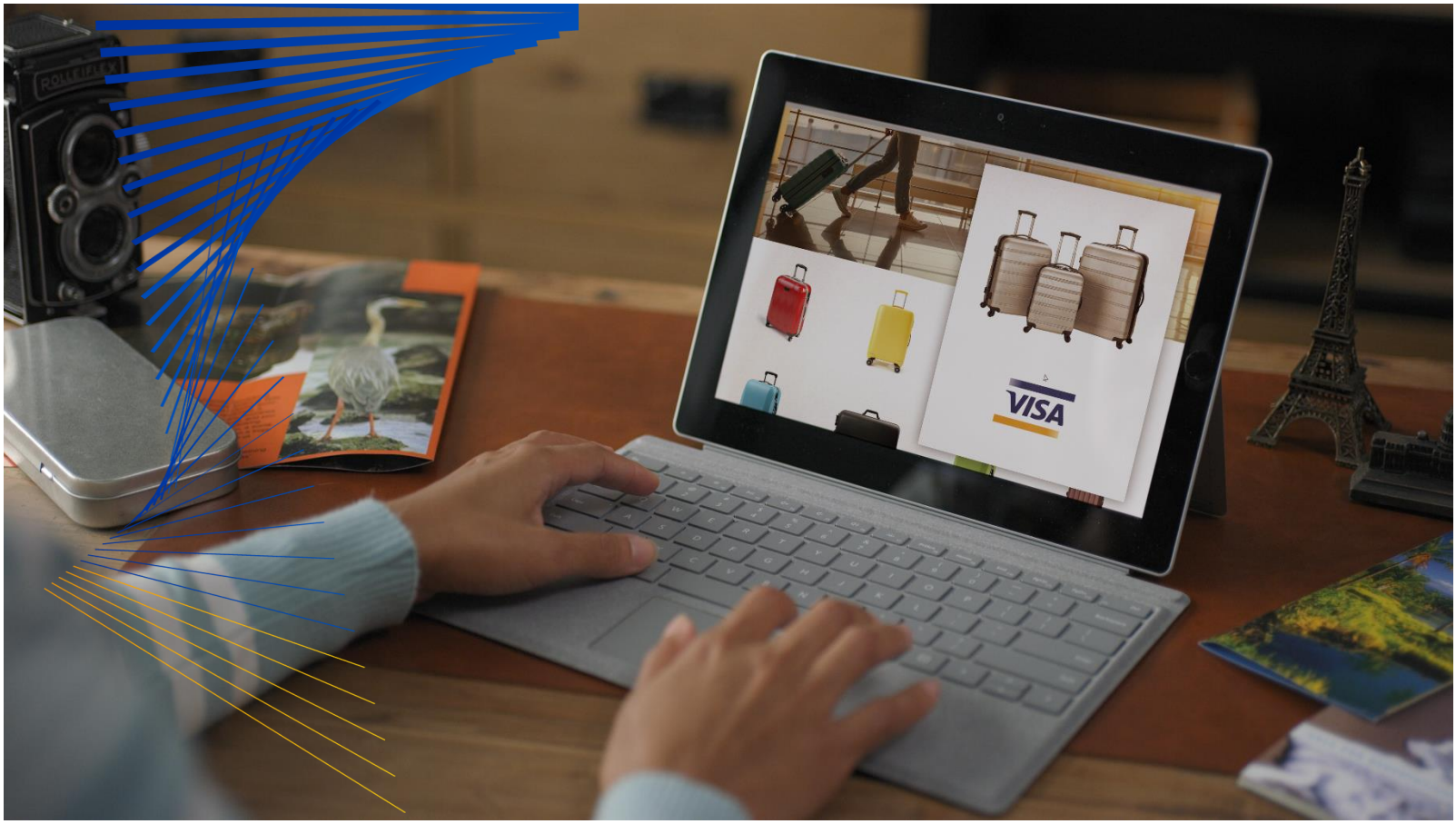


Merchant Bulletin

8th Edition

Key learnings and best practices post SCA enforcement in the European Economic Area

14 June 2021

Disclaimer

This communication is furnished to you solely in your capacity as a customer of Visa Inc. and/or a participant in the Visa payments system. By accepting this communication, you acknowledge that the information contained herein (the "Information") is confidential. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or as a participant in the Visa payments system. The Information may only be disseminated within your organization on a need-to -know basis to enable your participation in the Visa payments system. Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. The products and services described in this document may be subject to further development. Visa reserves the right to revise this document accordingly. As a new regulatory framework in an evolving ecosystem, the requirements for SCA still need to be refined for some use cases. This document represents Visa's evolving thinking, should not be considered as legal advice, and it is subject to change in light of competent authorities' guidance and clarifications. Visa reserves the right to revise this document pending further regulatory developments. This guide is also not intended to ensure or guarantee compliance with regulatory requirements. Payment Service Providers are encouraged to seek the advice of a competent professional where such advice is required.

Welcome

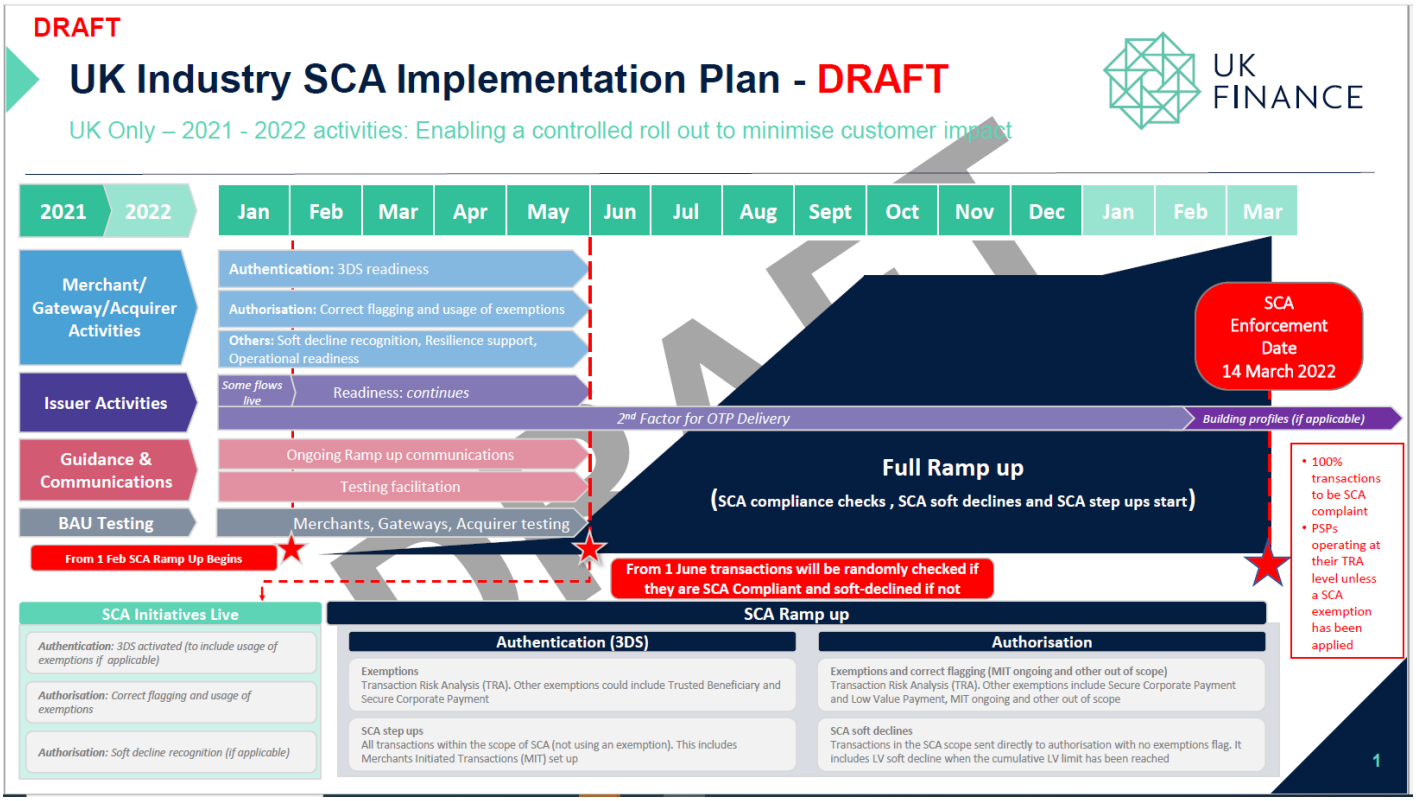
Welcome to Visa's eighth edition of the Merchant Bulletin. The purpose of this document is to support the payments ecosystem with latest progress with the enforcements of the Payment Services Directive 2 (PSD2) requirements for Strong Customer Authentication (SCA) in the European Economic Area (EEA) and how merchants, gateways and acquirers can follow best practices.

The seventh edition was published on 22 February 2021 focusing on PSD2 SCA implementation for e-commerce effective 1 January 2021 – in particular on key observations and learnings since the enforcement of PSD2 SCA in the EEA and guidance and best practices that can be implemented by merchants to avoid transaction declines and continue to provide best customer experience.

As all EEA markets have reached or will do so shortly, full SCA enforcement, we have summarised key emerging themes from a number of markets, feedback from issuers, remedies and best practices for merchants to effectively and successfully apply SCA and look ahead towards the UK ramp-up which started on 1st June.

UK ramp-up plan

The UK is the last European market to implement SCA. The UK SCA ramp-up plan commenced on 1st June 2021. At this point, UK issuers started to apply their SCA logic to a small percentage of transactions in both the 3DS and authorization flows. During the period of the ramp-up, merchants will notice a steady increase in 3DS challenges as well as soft declines for transactions that have not been correctly processed or flagged in line with SCA requirements.



The above SCA implementation plan is currently going through UK Finance's approval governance. The latest UK SCA ramp-up plan can be found here.

On Thursday 20 May, the Financial Conduct Authority (FCA) announced a further extension to the deadline for implementing SCA for e-commerce transactions to 14 March 2022. Their statement highlighted that the ramp-up from 1 June 2021 continues with the expectation that merchants are ready to process SCA compliant transactions from that date.

The full FCA announcement on the extension can be found here. Information on the 1 June 2021 ramp-up can be found here.

Merchant key entered transactions

Visa has observed that many merchants have manually key entered card data in their physical point-of-sale device or in a web interface for some transactions. Such transactions do not carry any authentication data and unless they carry some out-of-scope indicators, they will appear in-scope of the regulation and may be declined. On average, the approval rate on such transactions is just over 60%[1] (which varies widely by markets, issuers and merchants) and is expected to deteriorate as many issuers have complained that they have been "tolerant" but need to start declining those transactions. To avoid such declines, merchants who manually key enter transactions should contact their acquirers to discuss potential solutions as follows:

- **Merchants who key enter transactions because they were taken over the phone:**
  - These transactions are legitimate MOTO transactions and are out-of-scope of SCA. Merchants must ensure those transactions are indicated as MOTO as it has been observed that many are not.
    - It is possible that merchants' contracts with their acquirer did not include the handling of MOTO transactions. As the global pandemic has accelerated e-commerce and many merchants have started to utilised MOTO to deal with the demand. Merchants are advised to discuss with their acquirer what may be required so that orders taken over the phone can be correctly indicated as MOTO.
    - This may simply be due to the acquirer not flagging the transaction as MOTO due to a technical issue that needs to be corrected.
- **Many merchants in the travel & hospitality sector still key enter transactions originating from ecommerce bookings or card not present transactions after check-in.**
  - Systems must be upgraded to carry proof of authentication from the original booking in the Cardholder-Initiated Transaction message
  - Any card not present transactions added after the initial booking or after check-in must be processed as "Merchant-Initiated Transactions" when the cardholder is not available to initiate or authenticate.

[1] Source: Visa processed data

- If systems cannot yet be upgraded, acquirers can implement an interim solution for transactions originating from third party bookings by flagging the transaction as MOTO as long as SCA was carried out on the original booking.[2]

- **Some merchants key enter transactions when the chip card does not work:**
  - Merchants are reminded that in such cases a "fallback" option is needed, and as such, the transaction may be attempted via the magnetic stripe first. This is because, the issuer can recognise the transaction as a fallback and may decide to approve without authentication (to provide business continuity, but at the issuer's discretion). If the magnetic stripe does not work, only then can the merchant try the transaction via key entry but should be fully aware of the high possibility of declines due to the transaction looking non-compliant without SCA.

Issuers have been alerted of all the possible reasons why transactions may get to them as "key entered" and have been asked to consider regulatory requirements versus the desire to support business continuity/cardholder experience as well as apply regular risk-based analysis when deciding whether to accept or decline such transactions. They are also recommended to apply exemptions where applicable. However, as all markets ramp-up SCA implementation, merchants should expect increasing declines on those transactions and are thus encouraged to discuss as soon as possible the potential solutions with their acquirers.

Declines on transactions with differing authorization and authentication amounts

Merchants should be aware that submitting a transaction in authorization where the amount is higher than presented in the authentication request may result in an issuer decline as the transaction needs to be reauthenticated if the final amount is higher than the initially authenticated amount[3]. Visa has observed an increasing number of declines due to this issue.

- For transactions within the EEA[4], merchants should take great care in ensuring the authorized amount does not exceed the authenticated amount.

- While this is valid for any amount variation, Visa has observed many transactions where the authorization amount is greater than the authenticated amount by only a value of €/£0.01 and even if this amount variation is very low, issuers are declining those transactions.
  - Merchants are encouraged to check if they submit such transactions as it is suspected this may be due to system errors that may be corrected.
  - If this value is used with the intent to process an account verification transaction, merchants are reminded that account verification transactions can only be processed with a value of "zero"

---

[2] Contact your acquirer to access the detailed Visa Business news reference number: AI10295 "Preparing Travel and Hospitality Merchants for SCA Compliance on Indirect Sales Transactions", published in August 2020

[3] For merchants acquired in the UK, the FCA has indicated that it is sympathetic to an approach that allows the final amount to increase 20% above the authenticated amount so long as it is within reasonable expectations of the customer. Any amount variation would also have to be compliant with Visa Rules (a 15% variation is allowed, beyond this, merchants must follow the options described in section 4.2.2.3 of version 3 of *the PSD2 SCA for Remote Electronic Transactions—Implementation Guide*.

[4] Merchants acquired within the EEA and sending transactions to issuers within the EEA

currency unit. Any other value is not considered an account verification and thus can lead to SCA declines if no SCA or if the authorized amount is higher than authenticated amount.

- For cases where the final amount is higher than the authenticated amount, review the options available to handle such scenarios Visa has published, in section 4.2.2.3 of the ***Version 3 of the PSD2 SCA for Remote Electronic Transactions - Implementation Guide***. Contact your account executive or your acquirer to review the latest guide.

Resilience indicator

SCA for e-commerce has been enforced in the EEA since 1st of Jan 2021 and is live in most EEA markets. Any in-scope transactions that are not authenticated, and for which no exemption applies, are likely to be declined by issuers. This means in cases when a merchant, gateway, or an acquirer cannot enable SCA due to an outage in their authentication environment, up to and including the Visa directory server, all in-scope or non-exempt transactions during the outage may be declined.

Visa has introduced a new authorization indicator to be used by merchants to inform issuers when authentication was not performed due to this type of outage, providing a method of resiliency to the system when such an outage occurs. More specifically, the indicator means that an authentication outage occurred in the authentication flow between the merchant, gateway 3-D Secure (3DS) server, and directory server, which means an authentication request was not possible and an authentication response could not be received.

Usage of the resilience indicator in the authorization request is at acquirer liability (ECI 07) and there are conditions of usage, therefore all merchants must work with their acquirers to understand if they are able to use this indicator in the situation of an outage. Merchants must note that issuers may choose to not approve transactions with this indicator, and in such cases, merchants will need to do SCA once the connection is back.

The resilience indicator must not be used to indicate an outage in the issuer processing domain i.e. this indicator must not be used in cases where the ACS is unavailable. In situations where the ACS is unavailable, the Visa attempts server will continue to stand-in to provide an ECI 06.

While transactions containing this indicator do not represent transactions that can be considered exempt, or out-of-scope of the SCA regulation, the presence of the indicator enables the issuer to understand that this is a transaction where an authentication is expected but could not be performed due to an outage.

This provides issuers with the ability to explain to a regulator why they may have decided to authorize an in-scope transaction without authentication, on an exception basis, to support resiliency.

Merchant impact of 3DS 1.0.2 changes

In the seventh edition of the Merchant Bulletin, published on 22 February 2021, we communicated the upcoming global 'Changes to 3DS 1.0.2'. Please refer to that article as a reminder of the changes affecting 3DS1 this calendar year, ahead of full removal by 15 October 2022.

All merchants are strongly recommended to protect their future e-commerce business from being impacted by the changes to 3DS 1.0.2 by enabling their authentication solution on EMV 3DS ahead of 16 October 2021. EMV 3DS penetration of 3DS continues to grow at pace, as detailed in the EMV 3DS Performance section of this bulletin, with strong issuer adoption as well as optimal authorization approval rates.

From 16 October 2021 if an issuer chooses not to support 3DS 1.0.2, there will also be no Visa stand-in, which means no authentication is performed and the merchant retains fraud liability. Whilst the recommendation in Europe is for issuers to continue to support 3DS 1.0.2 beyond October 2021 due to the need to support SCA regulation, if a merchant relies only on 3DS 1.0.2 for their e-commerce authentication, then they should expect to see some issuers decommissioning the service from 16 October this year which will affect their online sales.

Visa will work with issuers on their schedule for the removal of 3DS 1.0.2, with the intention to minimize impact to payments, but it is strongly recommended that merchants act now to protect their future sales. More than 20% of European e-commerce transactions are routed through the authentication process and this has increased post PSD2 SCA enforcement. While each merchant's business is unique, being prepared to authenticate through EMV 3DS now will protect future e-commerce sales.

In addition to the changes from October this year, issues are already occurring which affect transactions where 3DS 1.02 is the authentication version. Merchants should be aware of the following two transaction scenarios, which require two factor authentication (2FA) under PSD2 SCA, noting that EMV 3DS is the only protocol that enables the merchant to request a 'mandatory challenge' to prompt the issuer to perform 2FA as required. Transactions where:

- A future payment mandate is being set up, or
- The issuer had responded with 'SCA Decline' in a direct to authorization - transaction have been identified as at higher risk of not completing successfully when 3DS 1.0.2 is used.

For both scenarios, a merchant must request a 'mandatory challenge' in the authentication flow, which is only possible in EMV 3DS. 3DS 1.0.2 does not identify to the issuer that 2FA is required and consequently the subsequent authorizations may be declined.

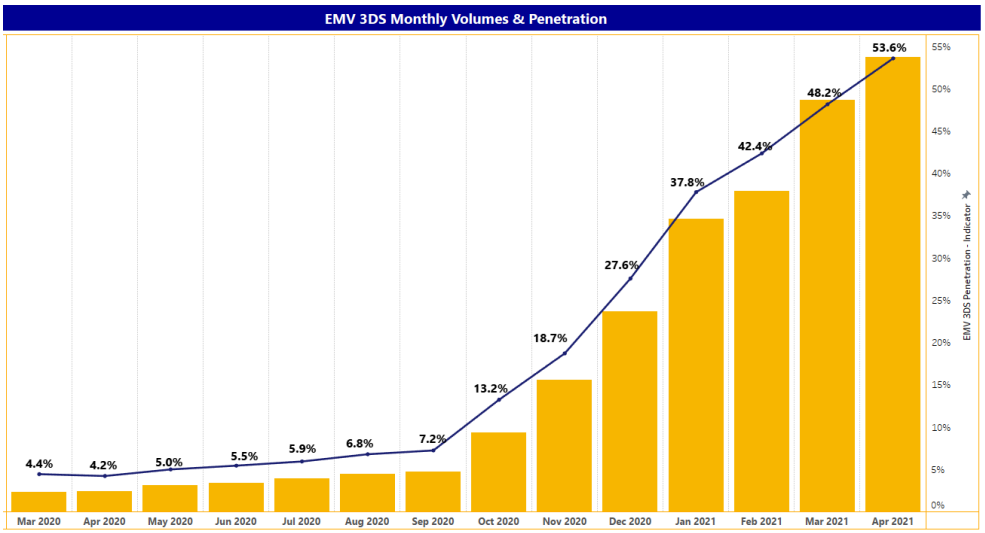
Merchants should speak to their acquirer, gateway and 3DS service provider immediately to plan their roadmap to EMV 3DS usage.

EMV 3DS performance

Enablement on EMV 3DS is in a very strong position, with ~99% of European PV enabled on general EMV 3DS, equalling 94% of the region's issuers. Visa is working closely with all European issuers to ensure that they fully enable on EMV 3DS, this is so merchants have the confidence to use 3DS with all their customers.

With issuers having fully enabled EMV 3DS portfolios on 2.1, attention is now being turned to the latest version of EMV 3DS 2.2 to maximise the capabilities and benefits that the new protocol offers. The proof in this is in the fact that enablement on EMV 3DS 2.2 has now surged to 83% of European PV, which is a ~45% increase since the last bulletin published back at the end of February.

With SCA being rolled out in the EEA and the UK, EMV 3DS offers the optimised framework to support dual-factor authentication. This has now become apparent in the data where EMV 3DS penetration of Total 3DS volumes is now at ~57% in Europe, a ~16% increase since the last bulletin.



As merchants continue to use 3DS for more of their e-commerce volumes, 3DS (ECI 5) approvals remain consistent and at a high rate of ~96%. Visa continues with its heightened monitoring and works closely with clients to ensure that their approval rates remain at the highest standard.

With so many issuers enabling EMV 3DS 2.2 capability, many are seeking EMV 3DS 2.2 ready merchants to live-prove their solutions. Merchants who would like to participate in testing with issuers are asked to contact Visa so that we can connect you to available issuers, please contact gctv3dsts@visa.com

The importance of flagging transactions correctly and including authentication data when required

Visa has observed several cases where the distinction between cardholder-initiated transactions (CITs) and merchant-initiated transactions (MITs) is not clearly indicated which has resulted in issuer declines. This is especially the case where merchants are processing Recurring, Instalment or Unscheduled Credential on file transactions. Merchants must review the below scenarios with their acquirer/gateway and ensure the intent of the transaction is accurately reflected by the use of correct flags. Failure to do so will result in unnecessary declines by issuers.

Use cases	Requirements
Cardholder is entering into a mandate (Recurring, Instalment or Unscheduled Credential on file) with the merchant.	• This is a cardholder-initiated transaction and must have SCA (no exemption can be used when setting up such an MIT mandate) • These transactions must have corresponding value (R, I or C) in POS Environment Code (F126.13) • No original transaction ID (F62.2 or F125*) is needed • The POS entry mode (F22) should be 01 if the card is key entered or 10 if the card was already previously on file
Merchant is processing an MIT (Recurring, Instalment or Unscheduled Credential on file) following a CIT	• SCA is not required on MITs as they are out-of-scope • These transactions must have corresponding value (R, I or C) in POS Environment Code (F126.13) • An original transaction ID (F62.2 or F125*) is required POS Entry Mode (F22) must be of value 10 as the card was stored on file.

Cardholder is agreeing to store card on file for CITs (no MIT Mandate is being setup at the same time)	• This is a cardholder-initiated transaction and must have SCA if there is a risk of fraud. • POS Environment Code F126.13 must have a value of 'C.' • No original transaction ID (F62.2 or F125*) is needed • As the card was not previously on file, the POS Entry Mode (F22) must not be 10. It must be 01 when key entered.
Cardholder is in session and is initiating a transaction with merchant where the card is previously stored on file (CIT)	• This is a cardholder-initiated transaction and SCA is needed unless an exemption applies. • POS Environment Code F126.13 must be blank. • No original transaction ID (F62.2 or F125*) is needed • POS Entry Mode (F22) must be of value 10 as the card was stored on file.

** Acquirers have the choice of submitting the Original Transaction Identifier either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Transaction Identifier in Field 125 to the issuers that participate to receive Field 125.*

For more information on Visa's MIT Framework, please contact your account executive or acquirer for ***Version 3 of the PSD2 SCA for Remote Electronic Transactions - Implementation Guide***. Note that the field names, numbers and values provided above are the ones that must be used by acquirers when sending authorization requests to Visa. Each acquirer/gateway may have their own specification to request this information from merchants so ensure to check with each their particular requirements to ensure each transaction can be appropriately populated in the Visa system.

Resources

Please see the SCA pages on your local Visa website for access to a range of resources: including infographics, merchant videos, and guides, click here for the UK SCA website.

What next?

The main messages to take away from this bulletin are:

1. Clearly indicate whether a transaction is cardholder vs merchant-initiated and include authentication data when it is required.
2. Many transactions are still manually key entered by merchants into POS without authentication data or out-of-scope indicators. Issuers that cannot apply an exemption have to decline these transactions to be SCA compliant. Merchants are strongly advised to work with their acquirers to ensure transactions are submitted correctly.
3. Enable EMV 3DS now to protect your business against the changes affecting 3DS 1.0.2 from 16 October 2021

Thank you for taking the time to read our Merchant Bulletin and please look out for the next edition that will be published in September 2021.