



PSD2 SCA Regulatory Guide

December 2020

Contents

Important Information	4
1. Purpose & Scope of this Guide.....	5
2. An Introduction to PSD2 Strong Customer Authentication (SCA)	6
2.1 The key provisions of the regulation	6
2.2 Timing of enforcement & national migration programmes.....	7
2.3 The requirement on Payment Service Providers, merchants and other parties to comply with the regulation.....	7
3. The application of SCA and use of factors	9
4. Dynamic Linking	13
4.1 Authentication codes and Dynamic Linking requirement.....	13
4.2 Meeting the requirements of Dynamic Linking.....	13
4.3 Meeting the requirement when the final amount is unknown.....	13
4.4 Variations in merchant name.....	14
5. Exemptions	15
5.1 Introduction.....	15
5.2 The Transaction Risk Analysis (TRA) exemption	16
5.3 The low value exemption	17
5.4 The trusted beneficiaries exemption	18
5.5 The secure corporate payments and protocols exemption	20
5.6 The contactless payments and point of sale exemption.....	22
5.7 The transport fares and parking exemption	23
5.8 The recurring payments exemption.....	23
6. Out of Scope Transactions	24
6.1 Introduction.....	24
6.2 Merchant Initiated Transactions (MITs)	24
6.3 Mail Order Telephone Order (MOTO)	27
6.4 One-leg-out (OLO)	27
6.5 Anonymous transactions.....	28
6.6 Other transactions that Visa considers do not require SCA by the cardholder	28
7. Delegated Authentication.....	29
8. Travel and hospitality and other complex use cases.....	31
8.1 The application of SCA to indirect bookings in the travel and hospitality sector....	31

9. Resilience	32
9.1 The Visa Attempts Server	32
9.2 Visa Resilience Indicator	32
10. Monitoring and reporting.....	33
10.1 Security & TRA exemption audits and reporting	33
10.2 Fraud monitoring & reporting	33
11. Confidentiality & integrity of customer security credentials.....	34
12. PSD2 SCA & GDPR	35
13. Bibliography	36
A Appendices	44
A.1 Appendix 7 EEA Countries in scope of PSD2 SCA	44

Important Information

© 2020 Visa. All Rights Reserved.

The trademarks, logos, trade names and service marks, whether registered or unregistered (collectively the "Trademarks") are Trademarks owned by Visa. All other trademarks not attributed to Visa are the property of their respective owners.

Disclaimer: 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.

As a new regulatory framework in an evolving ecosystem, the requirements for SCA still need to be refined for some use cases. This paper represents Visa's evolving thinking, but it should not be taken as a definitive position or 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 guide 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.

This document is not part of the Visa Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Rules, the Visa Rules shall govern and control.

References to liability protection, when used in this context throughout this guide, refer to protection from fraud-related chargeback liability under the Visa Rules.

Note on references to EMV 3DS, 3-D Secure 2.0 and 3DS 2.0: When in this document we refer to 3-D Secure 2.0 or EMV 3DS this is a generic reference to the second generation of 3-D Secure and does not reference a specific version of the EMVCo specification. Version 2.1 of the specification is referred to as EMV 3DS 2.1 and version 2.2 is referred to as EMV 3DS 2.2. Visa rules do not preclude Issuers and Acquirers agreeing alternative means of performing SCA.

Examples in this document show transactions processed through VisaNet. Visa supports the use of third party processors. Contact your Visa Representative to learn more.

1. Purpose & Scope of this Guide

The purpose of this guide is to summarise the main requirements of the PSD2 SCA regulation as it applies to electronic card payments and Visa's guidance on the practical application of SCA in a PSD2 environment.

The guide aims to provide a clear single point of reference providing guidance where:

- The text of the regulation does not expressly address a particular issue or is unclear in how it applies to a particular issue
- Visa believes it will be helpful to explain the basis for the practical PSD2 SCA solutions, rules and mandates it has put in place

The practical steps that Payment Service Providers (PSPs), merchants and other stakeholders need to take to optimize the application of PSD2 SCA along with details of Visa's PSD2 SCA solutions, rules and mandates are described in a series of Implementation Guides that are listed in the Bibliography section.

This guide is not intended to provide legal advice, ensure or guarantee compliance with regulatory requirements. Payment Service Providers and merchants are encouraged to seek the advice of a competent professional where such advice is required. **The following take precedence over content in this guide:**

- **Interpretations of the regulation and guidance provided by National Competent Authorities (NCAs)¹**
- **Visa rules**
- **Technical information and guidance published in EMVCo specifications, Visa specifications and Visa Implementation guides listed in the bibliography**

Visa recognizes that clients have choices and may wish to use alternative approaches, tools and services to those referred to in this guide.

¹ National Competent Authorities (NCAs) are the local payment regulators in each country

2. An Introduction to PSD2 Strong Customer Authentication (SCA)

2.1 The key provisions of the regulation

2.1.1 The requirement to apply SCA

PSD2 requires that Strong Customer Authentication (SCA) is applied to all electronic payments - including proximity and remote payments - within the European Economic Area (EEA²) and currently the UK³.

2.1.2 The definition of SCA

SCA requires the authentication of a payer based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is). Each of the two factors must be from a different category and must be independent, such that the breach of one does not compromise the reliability of the other. SCA solutions must be designed to protect the confidentiality of the authentication data.

2.1.3 General requirements to apply risk-based transaction monitoring

Payment service providers must have risk-based transaction monitoring mechanisms in place that enable them to detect unauthorised or fraudulent payment transactions. These must take account of a defined set of risk factors⁴.

2.1.4 Authentication codes and Dynamic Linking

Dynamic Linking must be applied to authenticated transactions, through the generation of an encrypted authentication code that links the authenticated transaction to the authenticated amount and the merchant. The amount being authenticated and the merchant name must also be communicated clearly to the customer.

2.1.5 Exemptions

The SCA mandate is complemented by some limited exemptions that aim to support a frictionless customer experience. These exemptions are summarised in Section 5.

2.1.6 Out of scope transactions

Some specific transaction types are "out of scope" of SCA and do not require the application of SCA, subject to certain qualifying conditions being met. These transactions are summarized in section 0.

² For more information on the territories the requirement applies to please see Appendix 1

³ After the end of the Brexit implementation period (from 1 January 2021) SCA requirements are expected to remain in force and will be defined in accordance with relevant technical instruments published by the FCA. These will be enforced in the UK from 14 September 2021

⁴ Listed in Article 2 of the SCA RTS

Each of the above requirements, along with Visa's view on the practical considerations arising are described in the following sections of this guide.

2.2 Timing of enforcement & national migration programmes

The requirement to apply SCA came into force on 14 September 2019. In relation to e-commerce, the European Banking Authority (EBA) has recognised the need for a delay in enforcement to allow time for all parties in the payments ecosystem to fully implement SCA and has set a deadline of 31 December 2020 by which time the period of supervisory flexibility should end. While the majority of NCAs will align with the EBA's guidance, PSPs should ensure they act in accordance with guidance or additional conditions imposed by local regulators. The UK's Financial Conduct Authority (FCA) will start to enforce the regulation for e-commerce transactions from 14 September 2021 (subject to compliance with phased implementation plans). The migration plans of PSPs, including the implementation and testing by merchants should also be completed by 31 December 2020.

The divergence in enforcement dates between the UK and EEA means there is likely to be a period from 1 January 2021 when cross border transactions between EEA states and UK may be considered One-Leg-Out.

National managed migration programmes are in place in a number of markets. Typically coordinated through payment industry associations and overseen by NCAs, these aim to ensure that all ecosystem players are ready to apply SCA to a timeframe agreed with the NCA. These programmes have established staged milestones for implementation of 3-D Secure and other key technical enablers such as soft declines and for industry and consumer communications programmes.

2.3 The requirement on Payment Service Providers, merchants and other parties to comply with the regulation

Regulated Payment Service Providers (PSPs) are responsible for the application of SCA and of the exemptions. In the case of card payments, these PSPs are Issuers (the payer's PSP) or Acquirers (the payee's PSP). PSPs are also required to:

- Meet certain general authentication requirements to monitor transactions for indicators of potential fraud
- Ensure that authentication credentials and solutions are provisioned, distributed, transmitted and revoked securely
- Measure and report fraud rates to NCAs

Under certain circumstances, PSPs may outsource the application of Transaction Risk Analysis (TRA) to qualifying third parties. For example, an Acquirer may outsource TRA to a qualified merchant to support the application of the TRA exemption.

PSPs may also, under certain circumstances, delegate the application of SCA to a qualifying third party, such as a merchant or wallet provider that has the capability to apply compliant SCA. This process is known as Delegated Authentication.

All merchants in the EEA and UK who process electronic transactions must be able to submit them for SCA ahead of the enforcement date. Any transactions that are submitted for authorization after the enforcement date, without SCA or without a correct exemption or out of scope indicator will likely be declined by an Issuer.

In order to correctly submit remote transactions, merchants must support 3-D Secure (3DS) or have access to an alternative means of authenticating remote transactions and should support certain indicators within authorization messages. In particular all parties in the payments ecosystem are strongly encouraged to support the most recent version of EMV 3DS which provides additional functionality to support SCA for remote payments. For proximity payments, merchant terminals must support Chip and PIN and defined contactless standards. More detail on these requirements can be found in PSD2 SCA Implementation Guides listed in the References Section.

3. The application of SCA and use of factors

SCA means the payer must be authenticated, normally by their card Issuer, using at least two independent factors, each of which must be from a different category of possession, inherence, or knowledge. Visa strongly recommends that participants in the remote payments ecosystem adopt EMV 3DS for authenticating cardholders and as a means to apply SCA. EMV 3DS is an industry standard protocol adopted by all major card schemes and serves as the mechanism for cardholder authentication at the time of an e-commerce purchase.⁵

Each factor may be proven through various different elements, for example a proof of possession of a securely preregistered mobile phone for possession, a fingerprint or other physical or behavioural biometric indicator for inherence, or a password for knowledge.

While the PSD2 allows for any combination of at least two factors, in Visa's view, the most practical SCA solutions will make use of:

- **Possession** as the **first factor**, and
- **Inherence** as the **preferred second factor**, or
- **Knowledge** as an alternative compliant, but much less satisfactory, factor

Figure 1: SCA factors for practical solutions



Biometrics are the simplest and securest way to apply SCA. They minimise checkout friction and many customers are familiar with them and find them attractive. EMV 3DS enables biometric authentication for example via a mobile banking app to provide an inherence factor. While knowledge factors are compliant from a regulatory perspective, they have a number of significant security and user experience disadvantages and their use should be avoided wherever possible.

⁵ For more detailed information on the use of 3DS please refer to Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure and Visa Secure Issuer Implementation Guide for EMV 3-D Secure

The SCA RTS and subsequent Opinion⁶ published by the EBA clarify which elements are allowable to prove each factor.

These are summarized in Table 1 below:

Table 1: Allowable elements to prove each factor

Possible inference elements	
Element	Compliant with SCA?
Fingerprint scanning	Yes
Voice recognition	Yes
Vein recognition	Yes
Hand and face geometry	Yes
Retina and iris scanning	Yes
Keystroke dynamics	Yes
Heart rate or other body movement pattern identifying that the PSU is the PSU (e.g. for wearable devices)	Yes
The angle at which the device is held	Yes
Device, payer, transaction and other contextual but non-biometric information currently transmitted using EMV® 3-D Secure	No
Memorised swiping path	No

Possible possession elements	
Element	Compliant with SCA?
Possession of a device evidenced by an OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	Yes
Possession of a device evidenced by a signature generated by a device (hardware or software token)	Yes
Card or device evidenced through a QR code (or photo TAN) scanned and read by a QR code reader that would read the QR code displayed on the card or on the device	Yes

⁶ Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 21 June 2019

App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device	Yes
Card evidenced by a card reader	Yes
Card with possession evidenced by a dynamic card security code	Yes
App installed on the device	No
Card with possession evidenced by card details (printed on the card)	No (for approaches currently observed in the market)
Card with possession evidenced by a printed element (such as an OTP list)	No (for approaches currently observed in the market)

Possible knowledge elements	
Element	Compliant with SCA?
Password	Yes
PIN	Yes
Knowledge-based challenge questions	Yes
Passphrase	Yes
Memorised swiping path	Yes
Email address or user name	No
Card details (printed on the card)	No
OTP generated by, or received on, a device (hardware or software token generator, SMS OTP)	No (for approaches currently observed in the market)

Key points to note are as follows:

- There are a number of allowable potential mechanisms for proving possession including use of an app, browser or exchange of cryptographic keys so long as a secure device binding process is used to ensure a unique connection with the authorised user's device is made
- Physical biometrics including retina and iris scanning, fingerprint scanning, vein recognition, face and hand geometry and voice recognition are acceptable as inherence elements
- A One-time passcode (OTP) can only be used to prove possession and must be used in conjunction with another permissible element from the category of inherence or knowledge
- An OTP can only be used where it proves possession of a device – for example it is received on a mobile phone associated with a SIM card or generated by an OTP generator that has been securely preregistered and associated with a payer. OTPs sent by email or selected from a pre-printed list or matrix are not compliant possession elements
- Card details printed on the card cannot be used to prove either possession or knowledge
- A behavioural biometric that identifies the specific authorised user is allowable as an inherence element so long as it relates to physical properties of body parts, physiological characteristics and behavioural processes created by the body. This could include identifying a user from the way they type and swipe, and/or the angle they hold a device
- Knowledge elements including PINs, passwords passphrases and knowledge-based responses to questions are allowable as knowledge elements

These points have significant implications for the deployment of practical SCA solutions that meet the requirements of the regulation, minimise fraud risk and minimise user friction and inconvenience. Specifically:

- Out of Band Solutions that rely upon a securely device bound mobile banking or authenticator app to prove possession alongside a biometric to prove possession can meet the requirements of the regulation
- Authentication solutions that use an SMS delivered OTP to supplement card data (with no other authentication factors) do not meet the requirements of the regulation
- While the EBA have said in their 2019 opinion that non-physical behavioural information (such as device, payer, transaction and other contextual information) transmitted through protocols such as 3DS cannot currently constitute a factor in its own right, this data which includes device, location and other transaction and contextual data used within a Risk Based Analysis approach, provides a proven, accurate basis for assessing fraud risk and has minimal user experience impact. In practical solutions, fraud protection can be maximised by combining behavioural biometric indicators with 3DS data. Issuers should therefore ensure that the

solutions they deploy make full use of all available data to minimise user experience friction and fraud while maintaining regulatory compliance

- Knowledge factors meet the requirements of the regulation and from a regulatory perspective could be used as a second factor alongside an SMS OTP or Out of Band app. Issuers considering this approach should take into account the negative user experience implications and security risks associated with use of knowledge factors

For more practical guidance on the selection of challenge solutions please refer to the *PSD2 SCA Challenge Design Best Practice Guide*.

4. Dynamic Linking

4.1 Authentication codes and Dynamic Linking requirement

The SCA RTS Dynamic Linking requirement requires that the payer is made aware of the amount of the payment transaction and of the payee and that the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction and that any change to the amount or the payee results in the invalidation of the authentication code generated.

4.2 Meeting the requirements of Dynamic Linking

Visa's EMV 3DS program, and Visa Token Service (VTS), deliver an authentication code - Cardholder Authentication Verification Value (CAVV) and/or Token Authentication Verification Value (TAVV) - which can be linked to the transaction.

Visa's view is that the authentication code requirement can be achieved by the sharing and validation of the CAVV or TAVV which gives cryptographic proof that the authentication completed successfully. Specifically CAVV v7 and TAVV v8 include the necessary elements to support dynamic linking. For more information on the use of the CAVV and TAVV please see *PSD2 SCA remote Electronic Transactions Implementation Guide*.

4.3 Meeting the requirement when the final amount is unknown

The EBA has confirmed that the final amount should not increase above the authenticated amount.⁷ Re-authentication is required for any increases above the authenticated amount.

The same does not apply where the final, authorized amount is lower than the authenticated amount. In these cases, no re-authentication is required.

There are use cases where the amount increases after checkout due to circumstances not initiated by, but pre agreed with, the cardholder (for example additional shipping costs, online grocery item substitutions) and when the customer will not be available to reauthenticate when the final amount is calculated.

⁷In the UK, the FCA has indicated that it is sympathetic to an approach that allows the final amount to increase above the authenticated amount so long as it is within reasonable expectations of the customer, but has not yet taken a final decision. If such an approach is permitted, any amount variation would also have to be compliant with Visa Rules.

The following options are open to merchants to mitigate the risk that a transaction will be declined due to failure to authenticate an increased final transaction amount. Each option has its own benefits/considerations:

- 1. Authenticate at the start for the highest estimated amount that would cover any anticipated amount variation.** Under this option, T&Cs covering how the final amount will be calculated and when the charges will be collected must be disclosed and agreed by the customer. To minimize the risk of abandonment due to confusion, the T&Cs should clearly communicate to the customer that:
 - a. They are being authenticated for a maximum amount
 - b. They will only be charged for what they purchase (which may be lower than the authenticated amount) and for any other relevant charges not yet known but pre-agreed (e.g. shipping and taxes)
 - c. No charges will appear on their card statement until the order is finalised
- 2. Process the additional unauthenticated amount as an MIT Incremental authorization.** Under this option, the initial authorization is processed as an "initial" amount which could be the known amount at time of checkout (recommended) or an estimate of the final amount. The additional unauthenticated amount is then processed as an MIT – Incremental. This requires that T&Cs covering how the final amount will be calculated and when the charges will be collected are disclosed to and agreed by the customer before the initial amount is authenticated and that the acceptance of the T&Cs and the initial amount transaction is authenticated with application of an SCA challenge.

In the event that the final amount is higher than the authenticated amount and the merchant had not planned for amount variation using either option above, the merchant must contact the cardholder to process the additional amount. Merchants cannot simply process an additional authorization with an SCA exemption indicator without the customer initiating a new transaction - even if a transaction for the additional amount would qualify for an exemption - because exemptions can only be applied to CITs. MITs cannot be processed without prior customer consent and authentication.

In some use cases, customers may be able to make changes to an order after they have checked out and authenticated, and these changes may increase the final amount that the merchant submits for authorization. Options for handling those use cases in the context of PSD2 SCA are described in the upcoming Version 3 of the *PSD2 SCA for Remote Electronic Transactions—Implementation Guide*.

Additional information may also be found in *Visa Business News Article ID: A110607 Expanded Eligibility for Estimated and Incremental Authorization in the EEA and UK to Support Amount Variation*.

4.4 Variations in merchant name

The EBA has confirmed⁸ that the information included in the authentication code does not necessarily need to be the full or exact merchant name but can be a unique identifier corresponding to the payee at authentication. As a unique identifier may differ to the merchant

⁸ Response to EBA Q&A 2019_4556

name at authorization, this implies that a variation between the merchant name/identifier at authentication and authorization is acceptable under Dynamic Linking.

Where there are differences to the merchant name between authentication and the final transaction submitted to authorization, Acquirers should ensure that there is a clear rationale for this. For example, the merchant name should be clearly recognisable as being the same merchant in both flows, but character for character matching should not be required.

For example, in Travel and Hospitality bookings, when a transaction is the result of a booking via an agent who initiates authentication on behalf of a third party merchant that subsequently requests authorization, the name in the authentication request may be that of the agent only, or that of the agent and the merchant, whereas the name in the authorization request may be that of the merchant.

5. Exemptions

5.1 Introduction

The SCA mandate is complemented by some limited exemptions that aim to support a frictionless customer experience when a transaction risk is low.

Under the regulation, the application of exemptions is restricted to regulated PSPs however merchants may also play an active role. They may, for example, work with their Acquirer to apply the TRA exemption, indicate that they would like Issuers to apply the trusted beneficiaries exemption and may flag to Issuers that a transaction qualifies for the secure corporate payments exemption.

Table 2 below summarizes which PSP is able to apply which relevant exemption for remote card transactions according to the regulation.

Table 2: Summary of who may apply an exemption

Exemption	Issuer	Acquirer
Transaction Risk Analysis (TRA)	Yes	Yes
Trusted beneficiaries	Yes	No
Low value transactions	Yes	Yes
Secure corporate payment processes & protocols	Yes	No
Contactless payments at POS	Yes	Yes
Unattended terminal for transport and parking	Yes	Yes

The Issuer always makes the ultimate decision on whether or not to accept or apply an exemption and may wish to apply SCA or decline the transaction.

5.2 The Transaction Risk Analysis (TRA) exemption

5.2.1 Introduction

The TRA exemption allows for certain remote transactions to be exempted from SCA provided a robust risk analysis is performed (based on the requirements in Article 18 of the SCA RTS), and the PSPs meet specific fraud thresholds. TRA is key to delivering frictionless payment experiences for low-risk remote transactions. Issuers and Acquirers can both apply the TRA exemption so long as they meet certain requirements, including that their fraud to sales rates are maintained within the specific fraud thresholds for remote card payments, set out in Table 3.

The SCA RTS⁹ also lays down minimum requirements for the scope of transaction risk monitoring that must be carried out by PSPs.

Table 3: Specific fraud thresholds for remote card payments

Transaction value band	PSP Fraud Rate
≤€100	13 bps / 0.13%
€100 ≤ €250	6 bps / 0.06%
€250 ≤ €500	1 bps / 0.01%

Visa considers the TRA exemption to be the most important exemption that should be considered first by PSPs for the transactions that qualify for it based upon the PSP's fraud rate.

The EBA has confirmed¹⁰ that only the PSP seeking to apply the TRA exemption needs to have a fraud rate within the reference fraud rate for the transaction value band. So, for example, an Issuer may apply the exemption to a transaction within a value band for which its fraud rate is below the reference fraud rate even if the Acquirer's fraud rate is above the reference fraud rate for that band, and vice-versa.

5.2.2 Calculating the fraud rate for qualification for the TRA exemption

The PSD2 regulation¹¹ requires that:

- The calculation of the fraud rate includes both unauthorized¹² transactions and fraudulent transactions resulting from the manipulation of the payer.
- The calculation is defined as the total value of unauthorized or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of transactions, whether

⁹ See Recital 14 and article 2 of the EBA *Regulatory and Technical Standards for Strong Customer Authentication*

¹⁰ EBA Q&A # 2018_4034: https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4034

¹¹ Refer to the EBA *Regulatory and Technical Standards for Strong Customer Authentication* and the EBA *Opinion Paper on the Implementation of the RTS on SCA and SCSC 13 June 2018*

¹² Note in this instance the term "unauthorized" is used in a regulatory context to indicate a transaction that has not been authorized by the payer, as opposed to a transaction that has not been authorized through the Visa system by an Issuer

authenticated with the application of strong customer authentication or executed under an exemption. This means that while transactions where an exemption applies should be included in the calculation, out of scope transactions (i.e. MITs, OLO and MOTO transactions¹³) should not be included in the calculation.

- The fraud rate is calculated on a rolling 90-day basis, using data from the previous 90 days.
- In order to apply the exemption, an Issuer or Acquirer is required to provide the competent authorities, upon request, with the methodology, model and fraud rates it is using for the application of the TRA exemption. Issuers and Acquirers will be required to monitor their fraud rates to continue to apply the TRA exemption and notify their competent authority if they go over the reference fraud rates.

The EBA has confirmed¹⁴ that PSPs should include all fraud, including transactions to which SCA has been applied and those where an exemption has been applied, irrespective of which PSP applied the exemption. Issuers should therefore include fraud on exempted transactions where both the Issuer and Acquirer have applied exemptions and vice-versa. In the interest of maximising use of exemptions and minimising unnecessary friction, Issuers are not recommended to blanket decline Acquirer TRA indicators. They should take a risk based approach and, where appropriate, accept the application of the exemption where it is indicated by the Acquirer.

5.2.3 The role of merchants in applying the TRA exemption

While merchants cannot apply the exemption under the regulation, an Acquirer may outsource the application of the TRA process to the merchant¹⁵. Application of the Acquirer TRA exemption can be flagged either through an indicator in the authorization message or through EMV 3DS 2.2¹⁶. Larger and enterprise merchants are encouraged to adopt proactive strategies using sophisticated risk tools to minimise fraud rates and take advantage of the ability to apply the Acquirer exemption and send transactions direct to authorization, to minimise the impact on customer experience and reduce authentication costs. While an Acquirer may outsource application of the TRA exemption to a merchant, it is still the Acquirer's reference fraud rates (rather than merchant-specific fraud rates) which determine whether the exemption can be applied.

Merchants who have undertaken TRA may also submit transactions via EMV 3DS 2.2 with the TRA exemption indicator when they believe it applies.

The Issuer will always take the final decision on whether to allow the TRA exemption to be applied to a particular transaction when it is indicated by the merchant or Acquirer.

5.3 The low value exemption

The regulation allows the Acquirer or the Issuer to apply the low value exemption so long as the value of the transaction is less than €30 and the number of transactions using this exemption since the last application of SCA does not exceed 5, or the cumulative value of

¹³ See sections 6.2, 6.3 and 6.4 for definitions of these out of scope transactions.

¹⁴ EBA Q&A 2019_4702: https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4702

¹⁵ (Reference: EBA: *Opinion Paper on the implementation of the RTS on SCA and CSC - June 2018*, para 47)

¹⁶ For more information on exemption indicators please refer to *PSD2 SCA for Remote Electronic Transactions Implementation Guide*

transactions using this exemption since the last application of SCA does not exceed €100. However, in the majority of cases PSPs should consider applying the TRA exemption rather than the low value exemption:

- Acquirer application of the low value exemption is not recommended as a first choice as the Acquirer has no view of the cumulative consecutive transaction and value counts and the transaction will need to be resubmitted via 3DS if either limit is breached.
- Issuer application of the low value exemption is only viable for transactions submitted direct to authorization as the Issuer ACS will not have visibility of the cumulative transaction count and value for transactions submitted via 3DS.

5.4 The trusted beneficiaries exemption

The trusted beneficiaries exemption allows for the cardholder to add a trusted merchant to a list of trusted beneficiaries held by their Issuer, completing an SCA challenge in the process. Further SCA application on subsequent transactions by that cardholder with the trusted merchant should generally not be required.

- Visa has developed the Visa Trusted Listing programme¹⁷ to provide Issuers, Acquirers, technology providers and Merchants with a framework to enable the application of the trusted beneficiaries exemption. Visa Trusted Listing enables customers to: Add a merchant to their Trusted List when making a purchase with a participating merchant. During the purchase, the merchant will send a request through 3-D Secure 2.2 for the Issuer to give the customer the option to add the merchant to their Trusted List.
- Add a merchant to their Trusted Listing outside of the purchase flow, for example when saving a card on file, or after the transaction completes. The merchant will send a request through 3-D Secure 2.2 for the issuer to give the customer the option to add that merchant to their Trusted List.
- Manage their Trusted List through their Issuer's online or mobile banking app. Customers can view the Trusted List, and add or delete merchants from their Trusted List.
- Make changes to their Trusted List via their Issuer's call centre to remove a merchant from their Trusted List.
- Remove a merchant when on the merchant's site (if supported by the merchant). The customer would navigate to the payment or wallet section where they are able to select an option to remove them from their Trusted List (the merchant will send a request through 3-D Secure 2.2 for the Issuer's ACS provider to confirm the customer would like to remove them).

Once a customer has added a merchant to their Trusted List, future purchase at that merchant would typically not require SCA.

5.4.1 Restrictions on the application of the trusted beneficiaries exemption

It should be noted that in order to be compliant with SCA provisions:

¹⁷ For more information, please refer to the *Visa Trusted Listing Implementation Guide v1.2 December 2020*

- Only Issuers can create/maintain lists of trusted beneficiaries on behalf of cardholders and use the trusted beneficiaries exemption (which Issuers may do through Visa Trusted Listing)
- Only customers can add or remove a merchant to/from a Trusted List
- Additions to, and amendment of, the Trusted List requires SCA
- Acquirers cannot apply this exemption and a merchant cannot set up the Trusted List for the purpose of the SCA exemption
- A payment transaction can only use the trusted beneficiaries exemption if the intended recipient of funds for the transaction is a merchant who is on the customer's list of trusted beneficiaries
- The customer may add or remove the merchant to or from their Trusted List through an Issuer controlled experience which requires SCA
- The trusted beneficiaries exemption cannot be applied to an agent or marketplace platform through which a customer is initiating transactions, when that agent or marketplace platform is not the merchant requesting authorization for those transactions, unless the merchant itself is on the cardholder's Trusted List. An example would be a travel agent taking bookings on behalf of third party suppliers such as hotels and airlines under a model where the customer pays the supplier directly. In that example, each supplier will need to be trusted separately.

Note the PSD2 regulation does not define a transaction value limit for the application of the trusted beneficiaries exemption so it can be applied to transactions of any value.

5.4.2 The allowable role of merchants and Acquirers in the application of the trusted beneficiaries exemption

While an Acquirer may not apply the trusted beneficiaries exemption, EMV 3DS 2.2 and the Visa Trusted Listing solution allow for:

- A cardholder to enroll a merchant in their trusted beneficiaries list while completing an SCA authenticated transaction; and
- A merchant to be advised by a cardholder's Issuer as to whether it is on a cardholder's list and, if so, to indicate to the Issuer that it would like the exemption to be applied.

5.4.3 Liability

5.4.3.1 Regulatory

The payee's PSP cannot apply this exemption; therefore, the Issuer is deemed to apply the exemption and is liable for fraud from a regulatory perspective, if an authorization was approved without appropriate authentication under the Visa Trusted Listing Program.

5.4.3.2 Disputes

If a merchant and its Acquirer participate in Visa Trusted Listing and choose to send the trusted beneficiaries exemption indicator, under the Visa Rules, the Issuer will retain dispute rights, just as they do today, since SCA is not performed on the transaction. If a merchant or Acquirer would like liability protection, they can choose to submit a 3-D Secure authentication request

to the Issuer who can then decide to perform SCA or apply an exemption if the transaction qualifies.

5.5 The secure corporate payments and protocols exemption

Under SCA-RTS Article 17, PSPs are allowed not to apply SCA for payments made by payers who are both legal persons and not consumers. This is only the case where the payments are initiated electronically through dedicated payment processes or protocols that are not available to consumers. Subject to the view of local regulators, these payments may:

- Originate in a secure corporate environment, including for example, corporate purchasing or travel management systems
- Be initiated by a corporate customer using a virtual or lodged card

In many cases it will not be possible to authenticate transactions originating in a secure corporate environment and requesting SCA may result in valid transactions being declined.

In order to apply the exemption, Issuers must ensure that, and NCAs must be satisfied that, the processes or protocols used guarantee at least equivalent levels of security to those provided for by PSD2. NCAs may have their own procedures or processes for assessing use of this exemption.

Issuers are encouraged to demonstrate to NCAs that applicable processes and protocols meet the requirements of the regulation and Visa recommends that Issuers liaise with NCAs over the procedure for this as required.

5.5.1 Interpreting the exemption

Subject to further regulatory guidance, Visa's view is as follows:

5.5.1.1 The exemption applies only to payers who are legal persons and not consumers

Under SCA-RTS Article 17, PSPs are allowed not to apply strong customer authentication for payments made by payers who are not consumers and are considered to be a "legal person".

Issuers should liaise with NCAs to ensure they understand the interpretation of this exemption in each relevant jurisdiction.

5.5.1.2 Card products to which the exemption may be applied

Visa considers that transactions made for business purchases:

- Using commercial virtual cards, or Central Travel Accounts (CTAs)/ lodged cards such as those used within an access-controlled corporate travel management or corporate purchasing system, could be within scope of the exemption
- Using physical commercial cards that are issued for use by individual employees of a corporate entity and that originate within a secure corporate environment, may qualify for the exemption
- Using personal cards that have been issued to an employee or contractor as a consumer do not qualify for the exemption even if the transactions are for business purchases; the cardholder is reimbursed by the organization on whose behalf the purchase is being made; and/or the purchase is initiated from within a secure corporate environment

5.5.1.3 The exemption does not apply to transactions using physical commercial cards outside a secure corporate environment

The use of physical commercial cards issued to employees for business expenditure in circumstances where a secure dedicated payment process and protocol is not used (e.g. where online purchases are made via a public website) would not fall within the scope of this exemption, and SCA would need to be applied, unless the transaction qualifies for another exemption or is otherwise out of scope of the SCA requirement.

5.5.2 Examples of secure dedicated payment processes or protocols

Examples of secure corporate environments include:

- Corporate Travel Management Companies (TMCs) that store commercial card details of client employees within secure profiles that are only accessible by authorized employees through a secure log-in process
- Corporate travel booking tools (CBTs) that are only accessible by authorized employees through a secure log-in process
- Corporate procurement systems that can be accessed by authorized employees through a secure log-in process

Transactions initiated from within such environments with eligible cards should qualify for application of the exemption, subject to individual NCAs being satisfied that the security requirements of the regulation are met.

5.5.3 Frameworks of Controls

The card payment schemes have worked with the travel and hospitality industry and industry associations (notably UK Finance) to develop a framework of controls to enable the exemption to be applied in the case of secure corporate environments that are not directly controlled by regulated PSPs. This framework is underpinned by:

1. Contractual obligations between parties in the ecosystem, notably between Acquirers and merchants; merchants and TMCs/CBTs and TMCs/CBTs and corporate customers to ensure that appropriate controls are applied to transactions to which the exemption may be applied
2. Monitoring that requirements are being adhered to and measurement of fraud rates by PSPs with remedial action being taken where fraud rates exceed TRA exemption fraud rates and/or increase
3. Scheme rules

Visa Rules are being updated to include security conditions that must be met if a merchant/Acquirer is to apply the Secure Corporate Payment indicator to a transaction originating from a secure corporate environment.

For more information, please see the forthcoming *Secure Corporate Payments Exemption Implementation Guide*.

5.5.4 Considerations for Issuers

Issuers seeking to apply the exemption on behalf of corporate customers who initiate transactions within secure corporate environments such as TMCs or Corporate procurement

systems should work with those corporate customers to assess the secure environments, ensure that required controls are being applied, work to ensure the relevant NCA's requirements for applying the exemption are met, and provide the required evidence to the NCA.

Additionally Visa considers that where virtual cards, lodged cards or Central Travel Accounts (CTAs) are used to make payments initiated within a secure environment such as an environment provided by a TMC or corporate purchasing system vendor, these transactions may qualify for the exemption so long as the NCA is satisfied that the requirements of the regulation are met for that solution, in accordance with the NCA's procedure for approving use of the exemption.

Issuers should also note that in the UK, the FCA requires Issuers to:

- Provide comprehensive assessments of their operational and security risks, and the adequacy of mitigation measures and control mechanisms implemented in response to those risks. The secure payment processes or protocols need to be included in this assessment. The timing and scope of these assessments should be discussed with local regulators, including how to comply where the processes and protocols are controlled by payers directly
- Ensure the process or protocol is subject to transaction monitoring (in line with SCA RTS Article 21), fraud prevention, security and encryption measures
- Ensure fraud rates are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction as set out in the annex of the SCA RTS

5.6 The contactless payments and point of sale exemption

SCA is not required for contactless payments at point of sale subject to the following conditions:

- The value of the transaction must not exceed €50 (or the local currency equivalent for non-Euro Zone markets); and either
- The cumulative monetary amount of previous consecutive contactless transactions without application of SCA must not exceed €150 (or the local currency equivalent for non-Euro Zone markets); or
- The number of consecutive contactless transactions since the last application of SCA must not exceed five.

Once the limit for the monetary amount or number of transactions without the application of SCA exceeds the selected limit by the Issuer, SCA must be applied and the count is reset to zero. The cumulative monetary amount and number of transaction limit is counted on the basis of transactions where this particular exemption was applied (i.e. not to transactions where a different exemption was applied to avoid applying SCA).

Issuers can select whether to apply the transaction count or cumulative monetary amount limit, but not both. An Issuer can decide which limit to apply for all transactions at the outset, or apply limits on a transaction by transaction basis.

If an Issuer chooses to apply one of the limits for all transactions, the other limit can be exceeded without the application of SCA so long as the chosen limit is not breached. So, if the

consecutive transactions limit is chosen, the cumulative €150 limit can be exceeded without the application of SCA so long as there have been no more than five consecutive contactless transactions since the application of SCA and vice versa. If an Issuer does not choose a limit to apply and applies the thresholds on a per transaction basis, they would need to simultaneously check whether either limit has been breached and apply SCA as soon as either or both limits are reached¹⁸.

Visa recommends the application of the cumulative monetary amount based approach to minimise the impact on customer experience. Application of the limits on a transaction by transaction basis is not recommended as it may confuse customers and result in SCA being required on a more regular basis.

Contactless limits may be applied at device/token level rather than account level.

5.7 The transport fares and parking exemption

Article 12 of the SCA RTS states that PSPs shall be allowed not to apply SCA, subject to compliance with the general authentication requirements laid down in Article 2, where the payer initiates an electronic payment transaction at an unattended payment terminal for the purpose of paying a transport fare or a parking fee.

5.8 The recurring payments exemption

Visa does not consider the recurring transactions exemption to be applicable to Visa card transactions. Visa's view is card transactions that would otherwise be covered by the recurring transaction exemption are typically Merchant Initiated Transactions (MITs) and are therefore out of scope of SCA. On this basis, Visa does not provide any indicator for the usage of the recurring transactions exemption.

¹⁸ Reference EBA Q&A # 2018_4225 https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4225 and EBA Q&A # 2018_4182 https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4182

6. Out of Scope Transactions

6.1 Introduction

The following types of transaction are out of scope of SCA and do not require the application of SCA so long as certain conditions are met.

- Merchant Initiated Transactions (MITs)
- Mail Order Telephone Order (MOTO)
- One-leg-out (OLO)
- Anonymous transactions

Each of these is covered in more detail below. Visa also considers that some additional specific transaction types do not require the application of SCA.

Note: Offline transactions, for example purchases on aircraft where there is no connectivity, are subject to SCA and cannot be considered to be out of scope.

6.2 Merchant Initiated Transactions (MITs)

6.2.1 Definition of an MIT

MITs are transactions of a fixed or variable amount and fixed or variable interval, governed by an agreement between the cardholder and merchant that, once set up, allows the merchant to initiate one or more subsequent payments from the card without any direct involvement of the cardholder. A transaction can only be an MIT if the user is not available to (I) initiate; or (II) authenticate. If the cardholder is available to either initiate or authenticate, the transaction is not an MIT.

Once the initial authenticated cardholder initiated transaction (CIT) that establishes the agreement has been completed, subsequent qualifying MITs are out of scope of PSD2 SCA and therefore do not require authentication.

6.2.2 Why MITs are out of scope

MITs are accepted as being out of scope of the PSD2 SCA because the regulation applies to transactions initiated by the payer and MITs are initiated by the payee.

6.2.3 Qualification criteria

In order for transactions to qualify as MITs, the following criteria must be met:

- A transaction can only be an MIT if the user is not available to (I) initiate; or (II) authenticate. If the cardholder is available to either initiate or authenticate, the transaction is not an MIT.
- An MIT can only be submitted after a previous CIT has been performed, with appropriate authentication, to establish the initial agreement with the cardholder. This CIT may be a zero value transaction.
- SCA must be applied to the initial CIT used to establish the agreement with the cardholder unless the initial transaction:
 - Was performed before the enforcement date of the regulation

- Is out of scope of SCA e.g. MOTO.

or one of the following exceptions applies:

- The transaction qualifies for the secure corporate exemption
- The transaction is a Resubmission or Reauthorization, **as defined under the Visa MIT framework**, and has been authenticated, or qualified for an exemption, when it was originally initiated by the cardholder
- The agreement should be clearly disclosed and clearly define the circumstances under which an MIT may be used, including but not limited to:
 - The timing and frequency of the transaction or the event that will trigger the transaction
 - The transaction amount or a description of how the transaction amount will be determined
 - Any other terms and conditions of the agreement, including, the expiration date (if any)
- SCA must also be applied when certain changes are made to the agreement, for example the cardholder wishes to use a different card or upgrades a subscription package. For merchant driven changes to payment terms, authentication is not required provided that the original agreement T&Cs and other cardholder communications clearly cover the eventuality of such changes. If not, SCA is required. Example changes include:
 - The price changes (e.g. due to inflation or other changes for example in the calculation method of the amount)
 - The date or frequency of payment changes (e.g., moving from a monthly to yearly billing model)

There may be exceptions to this if the agreement that has been previously accepted and authenticated by the customer allows the payee to make changes without the explicit consent of the cardholder.

6.2.4 Examples of transaction types that qualify as MITs

Typical use cases that may qualify as MITs include:

- Subscriptions
- Regular payments initiated by services providers such as utility and phone bill payments, insurance premiums etc.
- Installment payment plans for the purchase of goods or services
- Balance payments
- Incremental and delayed payments and collection of no show fees in travel and hospitality services

Visa formally defines the following types of payments as MITs under its MIT framework:

Table 4: Types of MIT defined in the Visa MIT Framework

MIT Types	Description
Installment/Prepayment	<p>Installment payments describe a single purchase of goods or services billed to a cardholder in multiple transactions over a period of time agreed by the cardholder and merchant.</p> <p>Prepayment is one or many payment(s) towards a future purchase of goods/services.</p>
Recurring	<p>Transactions processed at fixed, regular intervals not to exceed one year between transactions and representing an agreement between a cardholder and a merchant to purchase goods or services provided over a period of time. Note that a recurring MIT is initiated by the merchant (payee) not the customer (payer) and so is out of scope of PSD2. Recurring transactions that are in scope of PSD2 (and therefore may benefit from the recurring transaction exemption) are those that a customer (payer) initiates, e.g. standing orders set up from a bank account.</p>
Unscheduled Credential on File (UCOF)	<p>A transaction using a stored credential for a fixed or variable amount that does not occur on a scheduled or regularly occurring transaction date, where the cardholder has provided consent for the merchant to initiate one or more future transactions which are not initiated by the cardholder.</p> <p>This transaction type is based on an agreement with the cardholder and is not to be confused with cardholder initiated transactions performed with stored credentials (CITs are in scope of PSD2 whereas UCOF transactions are MITs and thus out of scope).</p>
Incremental	<p>An incremental authorization is typically found in hotel and car rental payment scenarios, where the cardholder has agreed to pay for any service incurred during the duration of the contract.</p> <p>Additionally, an incremental authorization may be used in transaction use cases where the final amount is not known at completion of the order, for example the purchase of weighed goods through an online grocery shopping service and/or product substitutions. If the actual final amount is higher than the authenticated / authorized amount, the additional amount may be authorized as an MIT—Incremental and no additional authentication is needed, as long as the final amount is within the terms and conditions agreed upon with the cardholder at mandate setup.</p>
Delayed Charges	<p>A delayed charge is typically used in hotel, cruise lines and vehicle rental payment scenarios to perform a supplemental account charge after original services are rendered.</p>
No Show	<p>A No-show is a transaction where the merchant is enabled to charge for services which the cardholder entered into an agreement to purchase but did not meet the terms of the agreement.</p>
Reauthorization	<p>A Reauthorization is a purchase made after the original purchase and can reflect a number of specific conditions. Common scenarios include delayed/split shipments and extended stays/rentals.</p>
Resubmission	<p>This is an event that occurs when the original purchase occurred, but the merchant was not able to get authorization at the time the goods or services were provided. Usage is limited to mass transit sector.</p>

6.2.5 Examples of transaction types that do not qualify as MITs

Processing a transaction with a stored credential does not necessarily qualify the transaction as out of scope or exempt from SCA.

Many CITs use stored credentials and are in scope of SCA. For example, so-called “one-click” transactions, or transactions initiated through apps used for booking ride sharing or cycle hire services, fuel purchases etc., that use stored credentials do not qualify as MITs. Each transaction must be evaluated according to its circumstances to determine if SCA is required.

6.2.6 Processing of MITs within Visa systems

Visa requires that MITs are correctly flagged using the Visa MIT Framework and that the transaction identifier (ID) of the initial CIT or a previous MIT (where permitted) is submitted with the indicator to provide an audit path back to the initial CIT. For details, please refer to *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

6.2.7 Recurring transactions and subscriptions

The SCA RTS includes an exemption for recurring payments which are defined as a series of transactions of the same amount and the same payee. Visa considers that all recurring and subscription type payments that are initiated by the payee only are MITs and are considered by Visa to be out of scope. The recurring payments exemption is not therefore supported in the Visa processing system.

6.3 Mail Order Telephone Order (MOTO)

Payments made through Mail Order/Telephone Order are out of scope and do not require the application of SCA. Note, “voice commerce” payments initiated through digital assistants or smart speakers via the internet are not classed as MOTO. In Visa’s view, transactions initiated via telephone through Interactive Voice Response (IVR) can be considered as telephone initiated and therefore MOTO. If the IVR is internet based, the transaction cannot be classed as MOTO.

6.4 One-leg-out (OLO)

It may not be possible to apply SCA to a transaction where either the Issuer or Acquirer is located outside the EEA or the UK¹⁹. However, SCA should still be applied to OLO transactions on a “best effort” basis. If the Issuer is not technically able to impose SCA, the Issuer is not obliged to decline. The Issuer should make their own approval decision based on risk and liability considerations.

A transaction at a merchant that is located outside the EEA or UK but that is acquired from within the EEA or UK is not classed as one-leg-out and is in scope of SCA.

From 14 September, equivalent SCA requirements will be enforced in the EEA and the UK, the result of which is that SCA can and should be applied by all parties for UK-EEA cross border transactions.

6.4.1 Identifying one-leg-out transactions

One-leg-out transactions can be identified by Issuer BINs and Acquiring Institution Country Codes in Authorization requests and an Acquirer Country Code (ACC) extension in EMV 3DS.

¹⁹ From 14 September 2021

For more details, refer to the *PSD2 SCA Remote Electronic Transactions Implementation Guide*.

6.4.2 Understanding best efforts

The EBA has set out that PSPs should make 'best efforts' to apply SCA to one leg out transactions:

- A transaction uses a card issued in the EEA or the UK, but is acquired outside the EEA or the UK. In this case the Issuer should decide whether to approve, challenge (where possible²⁰) or decline the transaction based on their risk assessment, the liability implications and the impact on the consumer experience.
- A transaction uses a card issued outside the EEA or the UK, but is acquired within the EEA or the UK. In this case, we would recommend that Acquirer s/merchants send transactions in an SCA compliant way, such as via 3DS, where the Issuer supports this. The Issuer is not obliged to apply SCA.

6.4.3 Cross border transactions and different national enforcement timelines

Different SCA implementation timescales and regulatory enforcement dates between countries means there is a risk that cross-border transactions may be declined due to SCA being required in one country but not the other.

From 1 January 2021 to 14 September 2021 SCA will be enforced in the EEA but will not be enforced in the UK. During this time the UK will be one-leg-out and SCA should be applied on a best efforts basis as described above. However, while EEA Issuers are not obliged to decline one-leg-out transactions without SCA, there may be a heightened risk of declines if UK-acquired merchants send transactions to EEA Issuers without SCA.

This may also be a risk if timelines diverge between other EEA member states. As of December 2020, The Banque de France has also announced a gradual enforcement based on soft declines to 31 March 2021, with a possibility of further gradual implementation to 31 June 2021. The Danish Financial Supervisory Authority has also announced a short transition with enforcement to commence from 11 January 2021.

To minimize the risk of declines, merchants acquired in regions where the regulator has implemented additional enforcement flexibility may therefore wish to consider implementing SCA and submitting transactions via 3DS in line with the EEA implementation timelines.

6.5 Anonymous transactions

Transactions through anonymous payment instruments are not subject to the SCA mandate. An example is transactions using anonymous prepaid cards.

6.6 Other transactions that Visa considers do not require SCA by the cardholder

In addition to the transaction types that are identified as out of scope in the regulation, Visa considers that SCA is not required to be performed by the cardholder for the following transaction types:

- Original Credit Transactions (OCTs) and refunds. These do not require SCA to be performed by the recipient of the funds (i.e. the cardholder)
- Zero value authorization/account verification requests

²⁰ When the transaction is submitted via 3DS

7. Delegated Authentication

The EBA has confirmed that PSD2 allows PSPs to outsource authentication to an entity to conduct SCA on their behalf:

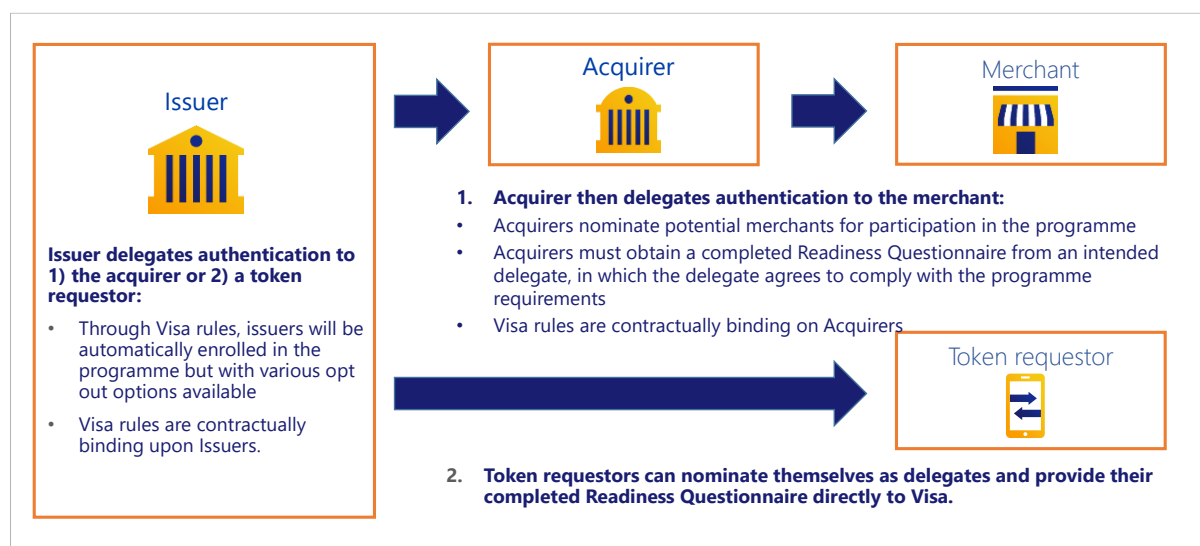
"...PSPs may outsource the execution of SCA to a third party. In that case, said PSPs should comply with the general requirements on outsourcing, including the requirements in the EBA Guidelines on Outsourcing."²¹

However, PSPs should be aware that they remain fully liable for their own regulatory compliance.

Visa has put in place a Delegated Authentication Program that provides a contractual framework to enable Issuers and Acquirers to delegate authentication to qualified delegates (such as merchants).




The program is designed to ensure Issuers and Acquirers have the practical information and legal tools to satisfy themselves that the regulatory requirements can be met.

Figure 2: How the Visa Delegated Authentication Program works



²¹ https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4047

Figure 3: The Visa Rules and Delegated Authentication implementation guide provide governance and controls

Issuer	Acquirer	Delegate
 <ul style="list-style-type: none"> • Receives notice of each delegate and responsible for any necessary regulatory notifications • Receives information about each delegate's authentication and monitoring approach, • Receives right of access and audit re. delegates' application of SCA • Required to maintain fraud and risk monitoring and may request additional SCA or decline if a serious risk is identified 	 <ul style="list-style-type: none"> • May choose to identify and nominate delegates for consideration for enrolment in the programme • Required to provide a Readiness Questionnaire completed by each potential delegate • Subject to the same monitoring responsibilities as issuers 	 <ul style="list-style-type: none"> • Required to complete a Readiness Questionnaire detailing their authentication and monitoring approach and agreeing to comply with the programme requirements • Required to meet fraud performance requirements upon entry and on an ongoing basis. • Required to apply SCA in line with all applicable regulatory requirements. • Required to flag to issuers at transaction level that SCA has been performed (not applicable for device-bound proximity payments)

Visa rules, implementation guide and Readiness Questionnaire place binding requirements on Issuers, Acquirers and merchants in relation to their role and obligations under the program.

Table 5: How tools within the Visa Delegated Authentication Program support PSP outsourcing obligations

Tool	How it supports outsourcing obligations
Readiness questionnaire	Provides the information and criteria to assess the suitability of potential delegates. Issuers will have visibility of questionnaires, which will enable them to keep regulators informed of delegations
	Comprises an agreement by the potential delegate to comply with the requirements of the program, including the implementation guide
Visa Rules & implementation guide	Set out the rights and obligations of all parties
	Provide termination and exit strategies
	Provide the Issuer with right of access and audit
Compliance program	Provides ongoing oversight and supervision of delegates

For more information, please refer to the *Visa Delegated Authentication Program Implementation Guide*.

8. Travel and hospitality and other complex use cases

SCA needs to be applied where required by the regulation. However, the communication of information relevant to the application of SCA and the exemptions is challenging for some payment use cases, notably in the travel and hospitality sectors where agent booking models and complex booking chains and legacy booking systems are commonplace.

Visa is working closely with industry bodies to ensure that solutions and approaches are available that allow the travel and hospitality sector to move to best practice. In some cases, this includes the implementation of interim operational solutions to allow authentication to take place and transactions to be processed without large scale declines in the short term.

8.1 The application of SCA to indirect bookings in the travel and hospitality sector

The Travel & Hospitality Sector is a highly complex eco-system comprising extensive legacy infrastructure, business models and service providers. Unlike other sectors, it relies heavily on indirect distribution channels.

There are many intermediaries in the sector between the agent handling the authentication and the merchant handling the authorization. These intermediaries to date have not been involved in the payment process beyond passing booking details and basic payment information. Under SCA, they are required to pass complex authentication data through the value chain. This requires systems upgrades to be undertaken by all intermediaries and by travel & hospitality merchants and this will not be completed and certified before the enforcement date.

The majority of the European travel industry comprises small businesses, notably in the hotel sector and many of these are unable to receive and pass proof of authentication data as they do not have integrated booking and payment systems.

The transactions originating from indirect channels are generally MITs and out of scope. The third party agent authenticates the customer and creates the MIT mandate at the time of booking and payment is taken by the merchant at a later stage where the customer is no longer 'on session' and not available to authenticate. However, in light of the operational challenges above, these transactions cannot currently be properly flagged as an MIT with proof of authentication, and therefore are likely to be declined.

Authentication must be performed, as required, by the regulatory enforcement date and several options exist to do this²². When the merchant wishes the agent to handle the authentication on their behalf and still process payment themselves, which is a key option for many merchants wishing to maintain current business models, an interim solution has been

²² Please see *Visa Business News: AI10295 Preparing Travel and Hospitality Merchants for SCA Compliance on Indirect Sales Transactions 20 August 2020* for more information

defined at ecosystem level²³ to enable these transactions to be flagged as out of scope even if proof of authentication is not yet available:

- As long as SCA has been applied (which is required unless the transaction qualifies for the secure corporate payments exemption), merchants in defined Travel & Hospitality Merchant Category Codes (MCCs) unable to receive authentication data or populate it in their authorization requests will be allowed to temporarily use an existing out of scope indicator (MOTO)²⁴ to flag these transactions as out of scope, until their chain of intermediaries and their own point of sale systems are updated

Visa is updating its rules to reflect the conditions for the usage of the MOTO indicator in the travel & hospitality sector as part of this interim solution. These rules aim to ensure the indicator is not abused and that use of the solution does not result in increased fraud. Improper usage will be subject to removal of the right to use the indicator. An end date after which the interim solution can no longer be used will be announced with a minimum one year's notice when there is an understanding of a realistic travel & hospitality ecosystem implementation timeline.

9. Resilience

Once the regulatory requirement for the application of SCA is enforced, any downtime or failure of systems that support the application of SCA, could result in transactions being declined. Visa offers the following solutions to support resilience in case of critical system failures or downtime:

9.1 The Visa Attempts Server

If for any reason an Issuer is unable to authenticate a transaction using 3DS, Visa will step in through the application of the Visa Attempts Server and respond with a CAVV and ECI value of 06. This can then be populated in the authorization message to indicate to the issuer that authentication was attempted but the issuer was unavailable to respond.

Issuers are recommended to have business continuity plans in place should they experience a critical system failure or downtime resulting in an ECI 06.

9.2 Visa Resilience Indicator

Effective January 2021, Visa is introducing a new authorization indicator in Field 34 that will enable Acquirers to flag that it is not possible to authenticate a transaction due to an outage in the 3-D Secure acceptance environment. Using this indicator is optional for Acquirers. Recognizing and acting on this indicator is also optional for Issuers. Both Acquirers and Issuers

²³ The interim solution has been developed and agreed through a UK Finance managed working group comprising the card schemes, payment industry representatives and merchants. This working group has had an EEA wide remit and the solution is applicable across Europe.

²⁴ Other schemes may also allow the use of an MIT indicator without proof of authentication for this purpose, this is not possible in the Visa system who will only use the MOTO indicator for this purpose.

need to consider regulatory requirements and resilience imperatives before deciding to use this indicator.

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 in the acceptance domain. 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 resilience.

On receiving a transaction flagged with this indicator, European Issuers that support it are recommended to use the value as part of their authorization response process considering it alongside other authorization decisioning factors.

For more information on these solutions please refer to *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

10. Monitoring and reporting

The regulation places a number of monitoring and reporting obligations on PSPs including:

10.1 Security & TRA exemption audits and reporting

The SCA RTS requires that the security measures implemented by PSPs under the regulation shall be documented, periodically tested, evaluated and audited and that PSPs applying the TRA exemption are subject to an audit of the methodology, the model and the reported fraud rates. The TRA exemption audit should take place on at least a yearly basis.

The SCA RTS requires that audit reports are made available to NCAs on request.

10.2 Fraud monitoring & reporting

Fraud monitoring and reporting requirements as required by the EBA are defined in the SCA RTS and the EBA Guidelines on fraud reporting under PSD2 (EBA/GL/2018/05) as amended by the *EBA Guidelines EBA/GL/2020/01*. Detailed processes for reporting are defined by individual NCAs.

10.2.1 TRA exemption monitoring and reporting

PSPs applying the TRA exemption must immediately report to the relevant NCAs where one of their monitored fraud rates exceeds the applicable reference fraud rate and must provide to the NCAs a description of the measures that they intend to adopt to restore compliance of their monitored fraud rate within the applicable reference fraud rates²⁵.

PSPs applying the exemption need to record and monitor the following information broken down by remote and proximity transactions:

²⁵ SCA RTS Article 20

- The total value of unauthorised or fraudulent payment transactions, the total value of all payment transactions and the resulting fraud rate, including a breakdown of payment transactions initiated with SCA and under each of the exemptions
- The average transaction value, including a breakdown of payment transactions initiated with SCA and under each of the exemptions
- The number of transactions where each of the exemptions was applied and their percentage in respect of the total number of transactions

Where a PSP's monitored fraud rate exceeds the reference fraud rate for a transaction value band for which it is applying the exemption, for two consecutive quarters, the PSP must immediately cease applying the exemption for that value band.

For information on the calculation of the fraud rate please see section 5.2.2.

10.2.2 Reporting of out of scope transactions

The EBA has confirmed²⁶ that Merchant Initiated Transactions and one-leg-out transactions initiated after 1 July 2020 need to be reported.

10.2.3 Reporting transactions submitted without SCA during the implementation period prior to regulatory enforcement dates

The EBA has confirmed that transactions initiated from 1 July 2020 but prior to the regulatory enforcement date that are submitted without SCA, but do not qualify for an exemption, should be reported, and has defined how these should be reported in Q&A # 2020_5070.

11. Confidentiality & integrity of customer security credentials

The SCA RTS²⁷ requires that PSPs take measures that protect the confidentiality and integrity of personalised security credentials, as well as authentication devices and software, to limit the risks relating to fraud. Notably, requirements on secure creation and delivery of personalised security credentials and their association with the payment service user, and conditions for the renewal and deactivation of those credentials. In relation to payments, these measures include:

- Security measures to protect the integrity of the transaction amount, the payee and the information displayed to the payer and authentication codes under Dynamic Linking²⁸
- Personalised security credentials are masked when displayed and are not readable in their full extent when input by the payment service user during the authentication

²⁶ For details, please refer to *EBA Q&A # 2019_4866*

²⁷ SCA RTS Recital 18, Article 1 and Chapter IV

²⁸ SCA RTS Article 5

- Personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in plain text
- Secret cryptographic material is protected from unauthorised disclosure
- The processing and routing of personalised security credentials and of the authentication codes take place in secure environments in accordance with strong and widely recognised industry standards²⁹
- PSPs ensuring that only the payment service user is associated, in a secure manner, with the personalised security credentials, the authentication devices and the software and that specific security requirements are met for the renewal, destruction, deactivation and revocation of personalised security credentials.³⁰

12. PSD2 SCA & GDPR

Visa's PSD2 solutions process data elements that are considered to be personal data under the GDPR. Merchants, Issuers and Acquirers should seek legal advice when considering the GDPR consequences of providing and processing data that may be considered to be personal information.

Specific principles to consider include:

- Lawful basis for processing: Merchants, Issuers and Acquirers should ensure they can rely on a lawful basis under the GDPR to process personal data in the context of Visa's PSD2 solutions. For most of these solutions, Merchants, Issuers and Acquirers may rely on legal bases other than consent including legal obligation, contract and legitimate interest for using personal data for fraud prevention purposes.
- Purpose limitation: Data provided by merchants for 3DS authentication must not be used for any purpose other than authentication and fraud prevention. Specifically, this data should not be used for sales, marketing or other purposes.
- Data storage and security: Merchants, Issuers and Acquirers should ensure that the requirements for data storage, security and international transfers under GDPR are applied to any personal data that is collected for Visa's PSD2 solutions.
- Transparency and Individual Rights: Issuers, Acquirers and Merchants should ensure that Terms and Conditions, Privacy Policies and Privacy Notices reflect the capturing and processing of data for fraud prevention purposes in the context of Visa's PSD2 solutions. This includes information on purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. In addition, Issuers, Acquirers and Merchants should ensure that they can respond to individuals' requests under the GDPR.

²⁹ SCA RTS Article 22

³⁰ SCA RTS Articles 24, 26, 27.

13. Bibliography

The following documents provide additional detailed guidance as described in the text of this guide.

Table 6: Bibliography

Document/Resource	Version/Date	Description
COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication	13 March 2018	The PSD2 SCA Regulatory Technical Standards (RTS) published by the European Banking Authority (EBA) that establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to comply with the security requirements of the PSD2 legislation.
Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC	EBA-Op-2018-04 13 June 2018	EBA opinion paper clarifying various SCA RTS requirements notably on the application of exemptions
Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2	EBA-Op-2019-06 21 June 2019	EBA opinion paper confirming 14 September 2019 as the date by which PSPs need to comply with the requirements of PSD2 SCA but introducing the option for NCAs to exercise supervisory flexibility, conditional on PSPs setting up migration plans and agreeing these plans with NCAs. The opinion also provides clarification on what may constitute a compliant element in each of the three possible categories of inherence, possession and knowledge, as well as additional requirements on dynamic linking and the independence of elements.
Opinion of the European Banking Authority on the deadline for the migration to SCA for e- commerce card-based payment transactions	EBA-Op-2019-11 16 October 2019	EBA opinion paper confirming that migration plans of all PSPs should be completed and supervisory flexibility should end on 31 December 2020

EBA Q&A		EBA Online Q&A Tool that provides answers to specific questions raised by interested stakeholders. This is available at https://eba.europa.eu/single-rule-book-ga/qna/view/publicId
PSD2 SCA for Remote Electronic Transactions Implementation Guide	Version 2.0 November 2019	Comprehensive Implementation Guide providing practical guidance on implementing SCA and Visa solutions. Version 3.0 to be published January 2021
Implementing Strong Customer Authentication for Travel and Hospitality	February 2019	An addendum to this implementation guide which provides merchants and Acquirers with examples of performing SCA across common payment use cases common in the travel and hospitality sectors.
PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements	Version 1.0 October 2019	Guide summarizing Visa Rules relevant to the application of PSD2 SCA. Version 2.0 to be published January 2021
PSD2 SCA Optimisation Best Practice guide	July 2020	This guide provides merchants, Acquirers and Issuers with guidance on minimising the number of transactions that will require Issuers to apply SCA challenges.
PSD2 SCA Challenge Design Best Practice Guide	July 2020	This guide provides merchants, Acquirers and Issuers with guidance on minimising friction when SCA challenges are required.
Secure Corporate Payments Exemption Implementation Guide	Q1 2021	Implementation guide providing more detailed guidance on the interpretation and application of the secure corporate payment processes and protocols exemption.
Visa Delegated Authentication Program Implementation Guide	Version 1.2 6 th November 2019	Describes the Visa Delegated Authentication Program and provides practical guidance to Issuers, Acquirers, technology providers, Delegates, and potential Delegates who participate in the Program on implementation and usage of the solution.
Visa Trusted Listing Program Implementation Guide	Version 1.2 December 2020	Describes the Visa Trusted Listing Program and provides practical guidance to Issuers, Acquirers, technology providers, and merchants who participate in the Visa Trusted Listing Program on implementation and usage of the solution.

Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure	Version 1.1, 21 August 2019	The Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure contains operational guidance for Merchants and Acquirers on the Visa implementation of 3-D Secure including:
Visa Secure Issuer Implementation Guide for EMV 3-D Secure	Version 1.1, 21 August 2019	The Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure contains operational guidance for Merchants and Acquirers on the Visa implementation of 3-D Secure including
Visa 3DS 2.0 Performance Program Rules	VBN 25th October 2018	Summary of Visa requirements and rules on Issuers, Acquirers and merchants for implementation of EMV 3DS
EMVCo 3-D Secure Specification	V2.2	Specification for the core 3DS technology that includes message flows, field values etc. available at: https://www.emvco.com/emv-technologies/3d-secure/
Visa Business News: Preparing for Strong Customer Authentication Enforcement in Europe	23 July 2020	VBN summarising key actions and milestones with the Visa ramp up plan in preparation for PSD2 SCA enforcement in the EEA.

Glossary

Table 7: Glossary of terms

Term	Description
1-9	
3-D Secure (3DS) 2.0	<p>The Three Domain Secure (3-D Secure™ or 3DS) Protocol has been developed to improve transaction performance online and to accelerate the growth of e-commerce. The objective is to benefit all participants by providing Issuers with the ability to authenticate customers during an online purchase, thus reducing the likelihood of fraudulent usage of payment cards and improving transaction performance.</p> <p>Visa owns 3DS 1.0.2 and licenses it to other payment providers. EMVCo owns EMV 3DS.</p> <p>Visa's offering of 3DS is called Visa Secure.</p>
3-D Secure Server (3DS Server)	A server or system that the merchant (or third party on the merchant's behalf) uses to support Visa's EMV 3DS Program authentication processing.
A	
Access Control Server (ACS)	A server hardware/software component that supports Visa's EMV 3DS Program and other functions. The ACS is operated by the Issuer or the Issuer's processor. In response to Visa Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the customer, and provides digitally signed authentication response messages (containing the authentication results and other Visa's EMV 3DS Program data) to the merchant.
Authentication	Authentication allows the Issuer to verify the identity of the cardholder or the validity of the use of the card, including the use of the cardholder's personalized security credentials and, where required, takes place before authorization, using the Issuer's selected authentication method, which in most cases will be 3-D Secure
Authorization	Authorization determines if a specific transaction request receives an approval or a decline from the issuing bank, or from VisaNet standing in on the issuing bank's behalf. Once a cardholder initiates a purchase, VisaNet informs the Issuer of the transaction, and receives back their approval or decline

Term	Description
	response. VisaNet then informs the requestor of the response, who passes the information along to the Merchant.
C	
Commercial Card	<p>A Visa Card or a Virtual Account issued to a Client Organization for business-related purchases, as specified in the Visa Rules, and associated with a BIN, account range, or an account designated as one of the following:</p> <ul style="list-style-type: none"> • Visa Corporate Card • Visa Business Card • Visa Purchasing Card
D	
Delegated Authentication	Issuers can delegate authentication to an Acquirer and in turn their qualified Delegates. Visa Delegated Authentication provides the framework and conditions for Issuers within the Visa ecosystem to delegate authentication to Delegates that meet stringent qualification criteria.
Device Binding	The process of verifying that the Issuer's cardholder has possession of the device on which the token is being used or provisioned to by performing Issuer authentication when the binding is established. Device binding also includes account binding by default. Device binding can occur during token provisioning or as a standalone action. Device binding links a token to a specific Token Requestor's device id and enables the linked device to satisfy the possession factor for SCA where the Token Requestor can reliably and unambiguously identify the device.
Directory Server (DS)	An EMVCo 3DS server component operated in the Interoperability Domain; it performs a number of functions that include: authenticating the 3DS Server, routing messages between the 3DS Server and the ACS, and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.
Dispute	A Transaction that an Issuer returns to an Acquirer.
Dynamic Linking	The process of associating the transaction to a payment amount and payee at the time of transaction processing

Term	Description
E	
Electronic Commerce Indicator (ECI)	A value used in an electronic commerce transaction to indicate the transaction's level of authentication and security.
Exemption	<p>The PSD2 SCA RTS provides a number of exemptions to SCA, which could result in minimizing friction and attrition in the customer payment journey. These are:</p> <ul style="list-style-type: none"> • Low value exemption • Recurring payment exemption • Trusted beneficiaries exemption • Secured corporate payment exemption • Transaction Risk Analysis
Exemption Threshold Value (ETV)	The maximum transaction value for which the TRA exemption may be applied, subject to the PSP's fraud rate being within the Reference Fraud Rate for that transaction value band. The ETV may also be thought of as the upper limit for each transaction value band shown in Table 3.
L	
Liability	Any and all damages (including lost profits or savings, indirect, consequential, special, exemplary, punitive, or incidental), penalties, fines, expenses and costs (including reasonable fees and expenses of legal and other advisers, court costs and other dispute resolution costs), or other losses.
M	
Merchant Initiated Transaction (MIT)	A transaction, or series of transactions, of a fixed or variable amount and fixed or variable interval governed by an agreement between the cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the cardholder. A transaction can only be an MIT if the cardholder is not available to (I) initiate; or (II) authenticate the transaction. If the cardholder is available to either initiate or authenticate, the transaction is not an MIT.
O	
Original Credit Transaction (OCT)	A Transaction initiated by a Member either directly, or on behalf of its Merchants, that results in a credit to a Visa Account Number for a purpose other than refunding a Visa purchase.

Term	Description
Out-Of-Band (OOB) Authentication	A Challenge activity that is completed outside of, but in parallel to, the 3-D Secure flow. The final Challenge Request is not used to carry the data to be checked by the ACS but signals only that the authentication has been completed.
P	
Primary Account Number (PAN)	The Primary Account Number (PAN) is the number embossed and/or encoded on payment cards and tokens that identifies the card Issuer and the funding account and is used for transaction routing. PAN normally has 16 digits but may be up to 19 digits.
Payment Facilitator	A vendor or service provider that is not a regulated Acquirer but is providing services on behalf of a merchant enabling that merchant to authenticate and/or accept electronic payments.
PSD2	The Second European Payment Services Directive whose requirements include that Strong Customer Authentication is applied all electronic payments where both Issuer and Acquirer are within the European Economic Area (EEA). This requirement is effective as of 14 September 2019 ³¹ .
PSP	In the context of PSD2, Regulated PSPs are responsible for the application of SCA and of the exemptions. In the case of card payments, these PSPs are Issuers (the payer's PSP) or Acquirers (the payee's PSP).
R	
Reference Fraud Rate (RFR)	The benchmark maximum fraud rate, defined by the PSD2 SCA RTS, that a PSP's calculated fraud rate must be equivalent to or below in order for that PSP to qualify to apply the TRA exemption to a transaction of a specified value. The PSD2 SCA RTS defines three reference fraud rates for three transaction value bands, each defined by an ETV.
Regulatory Technical Standards (RTS)	An RTS is a standard that supplements an EU directive. An RTS is developed for the European Commission, in the case of PSD2

³¹ The European Banking Authority (EBA) has recognized the need for a delay in enforcement to allow time for all parties in the payments ecosystem to fully implement Strong Customer Authentication (SCA). Merchants and PSPs should check with NCAs for enforcement timescales in their respective markets.

Term	Description
	<p>by the European Banking Authority (EBA) and is then adopted by the Commission by means of a delegated act.</p> <p>The PSD2 SCA RTS, (formally titled <i>Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication</i>) establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to comply with the security requirements of the PSD2 legislation.</p>
S	
Stored Credential	Information (including, but not limited to, an Account Number or payment Token) that is stored by a merchant or its agent, a Payment Facilitator, or a Staged Digital Wallet Operator to process future Transactions.
Strong Customer Authentication (SCA)	SCA, as defined by PSD2 SCA RTS, requires (among other things) that the payer is authenticated by a PSP through independent factors from at least two of the categories of knowledge, possession and inherence.
T	
Transaction Risk Analysis (TRA) Exemption	Under the Transaction Risk Analysis (TRA) exemption, PSPs may bypass SCA for remote transactions provided risk analysis is applied and the PSP's fraud rates, and transaction amounts are under certain thresholds (Article 18 of the PSD2 SCA RTS). The formula to calculate the PSP's fraud rate for the application of the TRA exemption is total value of unauthorized and fraudulent remote card transactions divided by the total value of all remote card transactions.
Trusted Beneficiaries Exemption	An exemption defined in the PSD2 RTS that allows, subject to certain restrictions, that a payer may add a trusted merchant to a list of trusted beneficiaries (Trusted List) held by their Issuer, completing an SCA challenge in the process. Sometimes referred to as "whitelisting".
Trusted List	A list of trusted merchants, or trusted beneficiaries, held by an Issuer on behalf of a customer. Sometimes referred to as a "whitelist"

A Appendices

A.1 Appendix 7 EEA Countries in scope of PSD2 SCA

The countries below represent those participating in the European Economic Area and therefore subject to PSD2 SCA regulation.

Table 8: EEA countries understood to be in scope of PSD2 SCA

AUSTRIA AT 040	ITALY IT 380
BELGIUM BE 056	LATVIA LV 428
BULGARIA BG 100	LICHTENSTEIN LI 438
CROATIA HR 191	LITHUANIA LT 440
CYPRUS CY 196	LUXEMBOURG LU 442
CZECH_REP CZ 203	MALTA MT 470
DENMARK DK 208	NETHERLANDS NL 528
ESTONIA EE 233	NORWAY NO 578
FINLAND FI 246	POLAND PL 616
FRANCE FR 250	PORTUGAL PT 620
GERMANY DE 276	ROMANIA RO 642
GREECE GR 300	SLOVAKIA SK 703
HUNGARY HU 348	SLOVENIA SI 705
ICELAND IS 352	SPAIN ES 724
IRELAND IE 372	SWEDEN SE 752

While the UK is no longer in the EEA, equivalent requirements apply in the UK and will be enforced for e-commerce from 14 September 2021.

Although not part of the European Economic Area (EEA), based on local law, strong customer authentication may apply to transactions in regions that are associated with countries within the EEA. Examples include micro-states and city-states in Europe, along with territories of EEA Countries outside of Europe. Clients in those regions should contact their local regulator to determine if SCA applies and if so how to comply and their Visa representative to determine how to optimize their performance of SCA.