



# PSD2 SCA for Remote Electronic Transactions Implementation Guide

January 2021

Version 3.0  
12 January 2021

**VISA**

# Contents

---

<b>Important Information .....</b>	<b>4</b>
<b>Using this document.....</b>	<b>5</b>
<b>1. Introduction: Visa’s guiding principles for PSD2 .....</b>	<b>8</b>
1.1 Introduction.....	8
1.2 Visa’s guiding principles.....	8
<b>2. The requirements of PSD2 Strong Customer Authentication and Visa’s interpretation .....</b>	<b>9</b>
2.1 The application of SCA and use of factors .....	9
2.2 Exemptions .....	12
2.3 Out of scope transactions.....	13
2.4 Dynamic linking .....	16
2.5 Visa PSD2 Solutions and GDPR.....	16
<b>3. Visa’s PSD2 solutions.....</b>	<b>18</b>
3.1 Solution summary.....	18
3.2 Authorization options.....	20
3.3 3-D Secure .....	41
3.4 Visa’s PSD2 solutions using Visa Token Service (VTS) .....	58
3.5 Visa Rules & policies for authentication & authorization under PSD2.....	62
3.6 Visa Trusted Listing .....	63
3.7 Visa Delegated Authentication .....	65
3.8 Visa Pre-dispute products.....	67
3.9 The Visa MIT Framework.....	69
3.10 Visa Biometrics.....	81
3.11 Visa Consumer Authentication Service.....	81
<b>4. Optimizing the payment experience under PSD2 .....</b>	<b>82</b>
4.1 Introduction.....	82
4.2 Key principles.....	83
4.3 Step by step guide to SCA optimisation .....	101
4.4 Liability for fraud-related chargeback.....	109
4.5 Additional guidance on application of the exemptions.....	112
4.6 Challenge Design Best Practice .....	121
4.7 Additional Guidelines for Issuers .....	125

4.8	EMV 3DS and authorization fall-back options.....	132
4.9	Visa Direct and SCA under PSD2.....	137
4.10	Visa Secure Remote Commerce/Click to Pay.....	139
4.11	Visa Secure Authentication Technology and non-Visa Transactions.....	139
<b>5.</b>	<b>Payment use cases and sector specific guidance for merchants and PSPs.....</b>	<b>140</b>
<b>6.</b>	<b>Bibliography.....</b>	<b>141</b>
<b>A</b>	<b>Appendices.....</b>	<b>154</b>
A.1	Appendix 1 The Stored Credential Framework.....	154
A.2	Appendix 2 STIP SCA Flowchart.....	155
A.3	Appendix 3 Merchant Initiated Transactions.....	156
A.3.1	Industry Specific Business Practice MITs.....	156
A.3.2	Incremental Authorization Transaction - Reason Code 3900 in Field 63.3—Message Reason Code.....	157
A.3.3	Resubmission Transaction—Reason Code 3901 in Field 63.3—Message Reason Code.....	157
A.3.4	Delayed Charges Transaction—Reason Code 3902 in Field 63.3—Message Reason Code.....	158
A.3.5	Reauthorization Transaction—Message Reason Code 3903 in Field 63.3—Message Reason Code.....	158
A.3.6	No Show Transaction—Reason Code 3904 in Field 63.3—Message Reason Code	159
A.3.7	Standing-Instruction MITs.....	159
A.3.8	Installment Payment Transaction and Prepayment (partial & full) Transaction — Value "I" in POS Environment Field 126.13.....	160
A.3.9	Recurring Payment Transaction —Value "R" in POS Environment Field 126.13 ....	160
A.3.10	Unscheduled COF Transaction —Value "C" in POS Environment Field 126.13	161
A.4	Appendix 4 EEA Countries in scope of PSD2 SCA.....	162
A.5	Appendix 5 Transaction assessment decision point considerations.....	163
A.5.1	Merchant/Acquirer decision points.....	163
A.5.2	Issuer decision points.....	170

# Important Information

---

© 2019 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. We encourage clients to contact Visa if they experience challenges due to conflicting guidance from local regulators. Where it makes sense, Visa will proactively engage with regulators to try and resolve such issues.

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 2.1.0 of the specification is referred to as EMV 3DS 2.1 and version 2.2.0 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.

# Using this document

---

This guide forms part of a set of Visa guidance documents that are relevant to the implementation of Strong Customer Authentication under PSD2. The guide is written for business, technology and payments managers responsible for the planning and implementation of PSD2 policies and solutions within Issuers, Acquirers, merchants, gateways and vendors. It aims to provide readers with guidance to support business, process and infrastructure policy decisions needed to plan for the implementation of SCA. It is supported by more detailed implementation guides and other documents that are listed in the bibliography in Section 6.

This guide covers remote electronic payments.

PSD2 SCA also applies to card present payments, including contactless payments and electronic payments made using devices including mobile handsets and wearables in a “face to face” environment. Please see *Visa Contactless and Card Present PSD2 SCA: A Reference Guide to Implementation* for more details.

This guide is structured as follows:

Section	Title	Description
1	Introduction: Visa’s guiding principles for PSD2	An overview of Visa’s guiding principles for PSD2 and corresponding focus for SCA
2	The requirements of PSD2 Strong Customer Authentication and Visa’s interpretation	Summarizing Visa’s interpretation of the PSD2 SCA requirements
3	Visa’s PSD2 SCA Solutions	Providing the essential information needed to interpret Section 4 of this document It details the range of tools and services Visa is making available to merchants, Issuers and Acquirers to optimize the application of SCA and allowable exemptions, including EMV 3DS, authentication and authorization message fields & values and Visa Rules
4	Optimizing the payment experience under PSD2 SCA	Providing information and guidance to help clients set their policies for application of SCA and exemptions. It describes the: <ul style="list-style-type: none"><li>• Key principles and considerations that govern authentication and authorization flows</li><li>• Options available for clients in terms of authenticating transactions and applying exemptions</li></ul>

Section	Title	Description
		<ul style="list-style-type: none"> <li>Considerations to take into account when deciding how to handle transactions</li> </ul> Guidance on managing of out of scope transactions and individual exemptions
5	Payment use cases and sector specific guidance for merchants and PSPs	This section is currently under review following EBA clarification that in payment use cases where the final amount is unknown, transactions must be reauthenticated if the amount increases above the amount initially authenticated. A short description of what to do in the meantime is provided. A revised version of this section will be included the next version (Version 4.0) of this guide.
6	Bibliography	A list of key additional reference documents
	Glossary	A glossary of terms used in the Guide
	Appendices	Additional technical detail supporting the main text

Each section, and subsection, has been highlighted to show its relevancy to each client stakeholder group. The icons used throughout this document are as follows:



## Important Note:

**This document provides guidance on the practical application of SCA in a PSD2 environment. Clients should note that this guide should not be taken as legal advice and the following take precedence over content in this guide:**

- **Interpretations of the regulation and guidance provided by National Competent Authorities (NCAs)**
- **Visa core 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.**

## Audience

This guide is intended for anyone involved in the initiation, application and processing of e-commerce transactions in the Visa Europe region. This may include:

- Merchants and their Acquirers and third party agents and vendors looking for guidance on implementing SCA solutions
- Issuers seeking to ensure that they accurately recognize transactions that are in and out of scope of SCA so they can maintain security without their cardholders' experience being unnecessarily disrupted

## Who to contact

For further information on any of the topics covered in this guide, Clients in the Visa Europe region may contact their Visa Representative or email [customersupport@visa.com](mailto:customersupport@visa.com).

Merchants and gateways should contact their Visa Acquirer.

## Feedback

We welcome feedback from readers on ways in which future editions of the guide could be improved. Please send any comments or requests for clarifications to [customersupport@visa.com](mailto:customersupport@visa.com).



# 1. Introduction: Visa's guiding principles for PSD2

---

## 1.1 Introduction

As the digital economy plays an increasing part in all our lives, it is vital that electronic payments are secure, convenient and accessible for all. Visa aims to provide innovative and smart services to Issuers, Acquirers and merchants, so they are able to deliver best in class payments to all Visa cardholders.

The Payment Services Directive 2 (PSD2) aims to contribute to a more integrated and efficient European payments market and ensure a level playing field for Payment Service Providers (PSPs). As such, it introduces enhanced security measures to be implemented by all PSPs.

## 1.2 Visa's guiding principles

Visa supports the PSD2 requirements for Strong Customer Authentication (SCA), and Visa programs and initiatives including 3-D Secure (3DS) and the Visa Token Service (VTS) may support PSPs to be PSD2 compliant. 3DS, along with our new products, programs and positions that are outlined in this paper, are in line with Visa's vision for secure, compliant, advanced and convenient electronic payments, and aim to deliver a good balance between security and consumer convenience. This will benefit all participants of the commerce ecosystem; reduced levels of fraud reduces cost for all parties, while merchants in particular will benefit from a lower friction payment flow that will increase conversion rates. Consumers will benefit from a low-friction purchasing experience, even when SCA is required.

Visa's guiding principles for PSD2 are:

- **Innovate** to give consumers choice and control to make informed decisions
- **Build** trust and security into every payment experience
- **Expand** access to data while keeping it protected
- **Foster** competition and innovation through open standards

Our Focus for SCA and ensuring that all players in the payment ecosystem are able to optimize both payment security and user experience are:

- **Leadership:** Provide clarity and education to the ecosystem
- **Products:** Build and evolve products and authorization messages
- **Programs:** Develop new programs and adjust rules as needed
- **Compliance:** Provide proof between parties to monitor performance





## 2. The requirements of PSD2 Strong Customer Authentication and Visa's interpretation

---

This section provides a brief summary of Visa's interpretation of the PSD2 Strong Customer Authentication (SCA) requirements.

PSD2 requires that SCA is applied to all electronic payments - including proximity and remote within the European Economic Area (EEA<sup>1</sup>); equivalent requirements apply in the UK.<sup>2</sup> The SCA mandate is complemented by some limited exemptions that aim to support a frictionless customer experience when a transaction risk is low. In addition, some transaction types are out of scope of SCA.

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. The migration plans of PSPs, including the implementation and testing by merchants should also be completed by 31 December 2020. While the majority of National Competent Authorities (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 which transposes PSD2 into UK law from 14 September 2021 (subject to compliance with phased implementation plans). The Banque de France has also announced a gradual enforcement of SCA based on increasing use of soft declines, to 31 March 2021 with potential for further gradual implementation to 31 June 2021.

Merchants and PSPs should check with NCAs for enforcement timescales in their respective markets.

### 2.1 The application of SCA and use of factors

SCA requires that the payer is authenticated by a PSP through at least two factors, each of which must be from a different category. These are summarized in Table 1.

---

<sup>1</sup> For more information on the territories the requirement applies to please see Appendix A.4.

<sup>2</sup> 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.

**Table 1: Strong Customer Authentication Factors**

Category	Description	Example
Knowledge	Something only the payer knows	A PIN code
Possession	Something only the payer has	A preregistered mobile phone, card reader or key generation device
Inherence	Something the payer is	A biometric (facial recognition, fingerprint, voice recognition, behavioral biometric)

Factors must be independent such that if one factor is compromised the reliability of the other factor is not compromised.

While the PSD2 regulation 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

The EBA Opinion published 21<sup>st</sup> Jun 2019<sup>3</sup> makes clear that:

- Static card details and security codes printed on a card cannot be used as either a possession or a knowledge element and the opinion advises competent authorities to closely monitor their application
- Dynamic card security codes may be used to provide evidence of possession and card security codes that are not printed on the card but sent separately to a customer could constitute a knowledge element
- An OTP cannot be used as a knowledge element but may be used to prove evidence of possession
- Inherence includes both biological and behavioural biometrics, where behavioural biometrics includes examples such as keystroke dynamics (typing and swiping patterns) and the angle at which the consumer holds the device.

The EBA also confirmed via their Q&A tool on 12 July 2020<sup>4</sup> that tokenised card details can be used to provide evidence of possession where the process of tokenisation binds the cardholder and the token to a preregistered device. Visa proposes - and has been engaging with regulators on - an SCA Authentication Factor Strategy that provides staged compliance and consumer choice by providing two primary, recommended authentication methods:

---

<sup>3</sup> Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 21 June 2019.

<sup>4</sup> [https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019\\_4827](https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4827)

### 2.1.1 Biometric plus device possession

Biometric authentication can be SCA compliant and a single device can provide both the possession factor (i.e. indicating possession of the device where the biometric is stored) and an inherence factor (the verification of the biometric captured). This approach has the additional advantages that:

- Consumers are getting more comfortable using biometrics
- Both Visa and MasterCard have requirements for Issuers to support biometrics
- The industry is aligned on this, and progress is underway

This method, also known as Out of Band (OOB) app plus biometric authentication uses a registered smart phone capable of supporting a relevant biometric (for example fingerprint or facial recognition) in conjunction with a mobile banking or other authentication app. The technology provides for two distinct and independent authentication factors, possession and inherence, both of which are facilitated using a biometric.

### 2.1.2 SMS OTP plus behavioural biometric

Behavioural biometrics can be used as a second factor (proving inherence) alongside OTP (proving possession) to provide an SCA solution that is significantly easier for customers to use and far more secure than OTP combined with a knowledge factor. This provides a potentially compliant evolution solution for existing single factor SMS OTP solutions that delivers a familiar and secure customer experience and is relatively straightforward for Issuers to implement.

Behavioural biometrics uses physical behaviour indicators that are unique to an individual customer. These can include the angle at which a device is held, the way keystrokes are entered, gesture analysis and swiping speed. Indicators are analysed and used to build dynamic user profiles and authenticate users.

The use of behavioural biometrics is in line with the EBA opinion on elements for SCA which identifies inherence elements such as keystroke dynamics (identifying a user by the way they type and swipe) and the angle at which the user holds the device.

A challenge solution that uses behavioural biometrics will help Issuers to be compliant with the regulation, while fraud protection can be maximised by combining the behavioural biometric indicators with EMV 3DS data, which include device, location and purchase history data, and provides a proven, accurate basis for assessing fraud risk.

### 2.1.3 Tactical and Inclusivity solutions

While biometrics based SCA solutions are recommended as the primary SCA solutions for the majority of customers, alternatives may be considered in the following circumstances:

- It is not possible for an Issuer to deploy one of the recommended solutions to all of its customers by the enforcement date and a Tactical Solution needs to be employed
- A minority of customers are unable or unwilling to access mobile phone based solutions and an Inclusivity Solution needs to be deployed

Tactical Solutions will normally use a knowledge element to provide second compliant factor alongside a possession factor provided either through an SMS OTP or a securely device bound banking authentication app.

Issuers need to focus on serving the majority of customers with the recommended SCA solutions, however Inclusivity Solutions should also be made available for limited deployment to those customers unable to access or use mobile phones for authentication. A number of two-factor options are available including card readers and hardware tokens that generate an OTP to prove possession of the device in response to entry of a knowledge factor such as a PIN.

## 2.2 Exemptions

The main exemptions to the application of SCA relevant to Visa e-commerce transactions are summarized below. It should be noted that not all exemptions are available to all PSPs. For more detail please refer to Section 4.5.

### 2.2.1 Transaction risk analysis (TRA)

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 2.

The SCA RTS<sup>5</sup> also lays down minimum requirements for the scope of transaction risk monitoring that must be carried out by PSPs.

**Table 2: 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%

### 2.2.2 Low value transactions

Remote transactions up to and including €30 do not require SCA so long as the cumulative number of previous remote transactions using the exemption does not exceed five, or the cumulative value of previous remote transactions using the exemption does not exceed €100, since the last application of SCA. Issuers should select either the cumulative or consecutive limit. If Issuers do not select a limit, they must apply both limits on a per transaction basis.

### 2.2.3 Trusted beneficiaries

Under the trusted beneficiaries exemption, once a customer performs SCA in order to add a qualifying merchant to their Trusted List, subsequent purchases with that merchant generally will not require SCA.

<sup>5</sup> See Recital 14 and article 2 of the Regulatory Technical Standards.

## 2.2.4 Secure corporate payments

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, lodged card or Central Travel Account, such as those used within an access-controlled corporate travel management or corporate purchasing system

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.

## 2.2.5 Recurring Transactions

Please note Visa does not support the recurring transactions exemption for 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.

## 2.3 Out of scope transactions

### 2.3.1 Transactions considered out of scope

The following transaction types 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)** - 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 subsequent payments from the card without any direct involvement of the cardholder. As the cardholder is not present when an MIT is performed, cardholder authentication is not possible. 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. An MIT can only be submitted after a previous cardholder initiated transaction (CIT) has been performed with appropriate authentication to establish the initial agreement with the cardholder specific to the MIT (even if that CIT is a zero-value transaction). Subsequent qualifying MITs are out of scope of PSD2 SCA and therefore do not require authentication.
- **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 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.

- **One-leg-out-** It may not be possible to apply SCA to a transaction where either the Issuer or Acquirer is located outside the EEA<sup>6</sup> or the UK<sup>7</sup>. However, SCA should still be applied to OLO transactions on a "best-effort" basis. Further text on one-leg-out transactions and best efforts is provided below. If the Issuer is not technically able to apply 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.
- **Anonymous transactions** - Transactions through anonymous payment instruments are not subject to the SCA mandate, for example anonymous prepaid cards. In the Visa system, these can include non-reloadable prepaid cards on which no KYC has been done and thus where the Issuer cannot authenticate the identity of the cardholder.<sup>8</sup>

### 2.3.2 Identifying one-leg-out transactions and understanding use of best efforts to apply SCA

The EBA has set out that SCA applies on a best-effort basis for one-leg-out transactions. We set out two scenarios below.

#### 2.3.2.1 Issuer within the EEA/UK, Acquirer outside the EEA/UK<sup>9</sup>

Where a transaction uses a card issued in the EEA or the UK, but is acquired outside of the EEA or the UK:

- If an Issuer receives a transaction request that does not enable them to apply SCA, the Issuer is not obliged to decline the transaction.
- The Issuer should make its own approval decision based on risk, customer experience and liability considerations.

#### 2.3.2.2 Acquirer within the EEA/UK, Issuer outside the EEA/UK<sup>9</sup>

Where a transaction uses a card issued outside of the EEA or the UK, but is acquired within the EEA or the UK:

- Visa recommends that Acquirers/merchants send transactions for authentication in an SCA compliant way, for example by submitting the transaction via 3DS, where this is supported by the non-EEA/UK Issuer.
- If a non-EEA/UK Issuer receives such a transaction request, it is not under any obligation to apply SCA.

---

<sup>6</sup> Refer to Appendix A.4 for a list of EEA countries.

<sup>7</sup> From 14 September 2021 (based on current enforcement plans).

<sup>8</sup> The fact that no KYC has been done and/or that it is a non-reloadable prepaid card will not necessarily mean the card is anonymous in all cases.

<sup>9</sup> Equivalent requirements are currently planned to be enforced in the UK from 14 September 2021.

### 2.3.3 Considerations arising from different SCA implementation timescales

Different SCA implementation timescales and regulatory enforcement dates between countries means there is a risk that cross-border transactions may be declined by an Issuer due to SCA being required in one country but not the other. This situation is effectively a transitional one-leg-out or one-leg-in scenario.

From 1 January 2021 to 14 September 2021 SCA will be enforced across most of the EEA but will not be enforced in the UK<sup>10</sup>. During this time, where one of the Issuer or Acquirer is in the UK and the other is in the EEA, these transactions may be considered 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. For example, as of December 2020, the Banque de France has announced a gradual enforcement based on soft declines to 31 March 2021, with a possibility of further gradual implementation to 31 June 2021.

Transitional risks that may arise and how they can be mitigated are set out below. Cross border transactions between the EEA and the UK are used as an example.

#### 2.3.3.1 Issuer within the EEA / Acquirer in UK (transitional one-leg-out)

There is a possibility that EEA Issuers may decide to request SCA on UK acquired merchants from 1 January 2021. In order to minimise the risk of declines, UK acquired merchants with customers using EEA issued cards may wish to consider implementing SCA and submitting transactions via 3DS in line with the EEA implementation timelines.

EEA Issuers are not obliged to decline transactions without 3DS (and where SCA is not otherwise technically feasible to apply) and during the transition period should treat them as described in section 2.3.2.1

#### 2.3.3.2 Acquirer within the EEA, Issuer within the UK (transitional one-leg-in)

In this case, prior to enforcement, the UK Issuer is not required to support SCA and the EEA merchant/Acquirer should consider whether to send transactions for authentication, via 3DS, only when they know the UK Issuer can accept them<sup>Error! Bookmark not defined.</sup>.

UK merchants acquired in the EEA will need to implement SCA in line with implementation and enforcement timescales in the Acquirer's region/market.

In practice, in addition to any regulatory requirements, Visa requires that all EEA and UK Issuers support EMV 3DS in any event from October 2020 as described in section 3.3.2.

---

<sup>10</sup> From 1 January 2021, pending any further developments, the UK could become a third country for the purpose of PSD2 SCA. Equivalent requirements to PSD2 SCA for e-commerce are currently planned to be enforced in the UK from 14 September 2021.

## 2.4 Dynamic linking

For electronic remote payment transactions, where PSPs apply SCA, both the amount and the payee must be clear to the payer when they authenticate a purchase. An authentication code must be produced but does not need to be visible to the cardholder.

Visa's programs such as 3DS, 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. The authentication code accepted by the PSP that is processing the transaction must correspond to the amount and payee. Visa systems enable the authentication code to be linked back to the amount and payee.

The regulation requires 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.

When the final amount is unknown, the EBA has confirmed that the final amount should not increase above the authenticated amount.<sup>11</sup> 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.

If the amount is higher, several options exist to handle amount variation. One of them is that the merchant may wish to set up an MIT to allow incremental amounts to be taken if the authorized amount is insufficient, rather than seek further authentication from the cardholder.

With regard to variations in merchant name, the EBA has confirmed<sup>12</sup> that the information included in the authentication code does not necessarily need to be the full or exact merchant name, and that while the RTS 'Regulation does not specify how the payee should be identified for the purpose of the dynamic linking requirements, it can be a unique identifier corresponding to the identity of the payee agreed to by the payer. The identifier agreed to by the payee at authentication may differ to the merchant name at authorization. For example:

- When there is a difference in the name used to identify a merchant between authentication and authorization such as use of a trading name vs. a legal entity name, use of different abbreviations or acronyms or a combination of the Acquirer and merchant name vs. the merchant name.
- 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.

For additional guidance on managing variations in merchant name and amounts within the constraints of these requirements please see section 4.2.2

## 2.5 Visa PSD2 Solutions and 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

---

<sup>11</sup> Response to EBA Q&A 2020\_5133.

<sup>12</sup> Response to EBA Q&A 2019\_4556.



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.

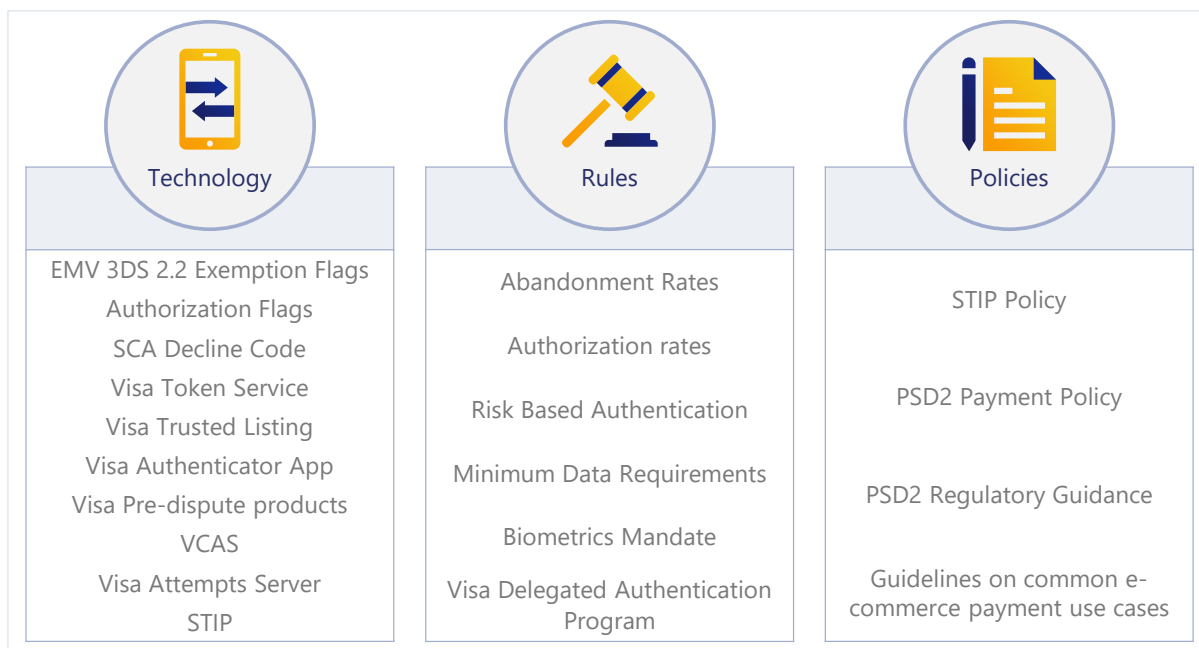
# 3. Visa's PSD2 solutions

## 3.1 Solution summary



Visa is implementing a portfolio of solutions to help support the application of SCA and exemptions. These comprise a combination of technology solutions, enhanced rules and policies which are summarized in Figure 1 below.

**Figure 1: Summary of Visa's PSD2 solutions**



The technology-based solutions include a suite of new products and programs that will support the application of SCA and exemptions. These are all based on a core set of foundational security technologies, illustrated in Figure 2 below.

**Figure 2: The foundational and SCA products & programs**

Foundational products and programs	SCA products and programs
 <p><b>Predictive analysis</b></p> <ul style="list-style-type: none"> <li>• Dynamic modelling based on current fraud trends, geographies and segments to effectively manage risk</li> <li>• Models built and maintained by Visa and refreshed every 12 months</li> </ul>  <p><b>3-D Secure</b></p> <ul style="list-style-type: none"> <li>• Industry standard for authentication</li> <li>• EMV 3DS has an enhanced user experience, expanded device usage, greater data sharing and is regulatory smart</li> </ul>  <p><b>Tokenization</b></p> <ul style="list-style-type: none"> <li>• Protecting payment data by replacing traditional card account numbers with a unique token that can be restricted by device, merchant or channel</li> </ul>	 <p>• Visa Pre-dispute Products</p>  <p>• Visa Trusted Listing</p>  <p>• Visa Delegated Authentication</p>  <p>• Visa Authenticator App</p>  <p>• Visa Consumer Authentication Service (VCAS)</p>

The application of SCA and the approval of transactions depends on two processes:

- **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. Where authentication is required, it takes place before authorization, using the Issuer’s selected authentication method, which in most cases is facilitated through 3-D Secure.
- **Authorization:** Is a separate process used by a card Issuer to approve or decline a Visa payment transaction submitted by a merchant/Acquirer or other card acceptor.

In a standard flow, merchants will submit a transaction for authentication, in some cases with an indicator requesting an exemption from SCA requirements. If the authentication is successful, the result will be returned along with a cryptogram (CAVV), and the merchant will submit the transaction to authorization along with the cryptogram and the correct indicators.

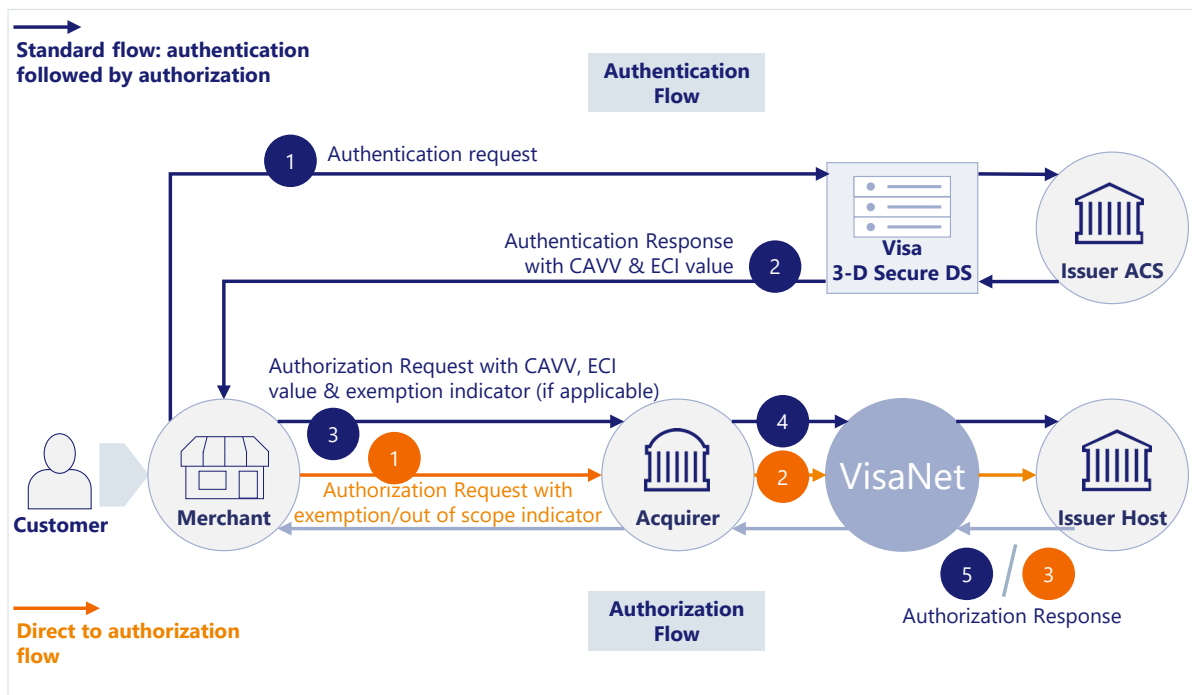
Visa also supports the option for transactions to be submitted direct to authorization, with an appropriate indicator. This may occur when:

- A transaction is out of scope of SCA
- An Acquirer applies an exemption such as TRA
- A qualified delegate has undertaken authentication under the terms of the Visa Delegated Authentication Program
- A merchant and the Issuer participate in the Visa Trusted Listing Program, the merchant is on the customer’s Trusted List, and the transaction qualifies for the trusted beneficiaries exemption

Factors to consider when selecting the appropriate option are summarized in section 4.3.

These basic flows are summarized in Figure 3 below:

**Figure 3: Simplified summary of authentication and authorization flows**



The following sections describe the authorization and authentication technologies and indicators offered by Visa.

## 3.2 Authorization options

### 3.2.1 Overview



Indicators in the authorization request message will be used by Issuers to identify:

- Transactions that are identified by merchants as being out of scope
- Acquirer exemptions (TRA and low value)
- Issuer applied exemptions that can be indicated by the merchant or Acquirer (trusted beneficiaries and secure corporate payments)
- That authentication has been applied under the Visa Delegated Authentication Program
- That authentication was not possible due to an outage in the acceptance domain
- There was no connectivity at the time of authorization

If a merchant would like to indicate that an Acquirer exemption is to be applied, an exemption indicator should be submitted in the authorization request. If the transaction is out of scope, the merchant must also ensure that the correct data is used to identify that it is out of scope.

### Key Point

Indicators in the authorization request message can be used by merchants to indicate certain out of scope transactions and exemptions. Merchants must ensure that the correct mechanism and indicators are used to identify exemptions being requested and transactions that are out of scope of SCA.

This section describes the Visa authorization message flows and fields and how these are used to support the application of exemptions and management of out of scope transactions.

### 3.2.2 Authorization message flows and fields



The main messages in the authorization flow are the Authorization Request and the Authorization Response messages. These enable merchants and Acquirers to request transaction authorization and Issuers to respond with the authorization result. The Electronic Commerce Indicator (ECI) value and CAVV (or TAVV if using the Visa Token Service (VTS)<sup>13</sup>) cryptograms are used to communicate the authentication status of the transaction. The messages work as summarized in Figures 4 and 5:

**Figure 4: Authorization request message (transaction authenticated via 3DS)**

Acquirer / Acquirer Processor	VisaNet
<ul style="list-style-type: none"> <li>Creates the authorization request including:               <ul style="list-style-type: none"> <li>The ECI, CAVV and/or TAVV</li> <li>MIT indicators if the transaction is an MIT</li> <li>Using appropriate MOTO indicating data if transaction is MOTO</li> <li>Exemption flag if exemption is being used</li> </ul> </li> <li>Forwards the authorization request to the Issuer through VisaNet</li> </ul>	<ul style="list-style-type: none"> <li>Recognises ECI 05 and 06 as EMV 3DS transactions and where a CAVV is present (for ECI 05, 06 and sometimes present for 07*), - either:               <ul style="list-style-type: none"> <li>VisaNet verifies the CAVV and send the issuer the CAVV verification results, or</li> <li>VisaNet forwards the CAVV to the Issuer to verify</li> </ul> </li> <li>Includes the 3DS Indicator to the Issuer in the authorization request, if the Issuer has elected to receive it</li> <li>Verifies the TAVV and sends the issuer the TAVV verification results</li> <li>Forwards the authorization request to the Issuer Host for processing</li> </ul>

\* Note: when an Acquirer TRA exemption request is accepted by the Issuer's ACS without the application of SCA by the Issuer the transaction will proceed as ECI 07 with a CAVV present.

<sup>13</sup> For more information about the Cloud Token Framework see Section 3.4.2; about Visa Delegated Authentication Program see Section 3.7; and about authentication data if using 3-D Secure see Section 3.3.8.

**Figure 5: Authorization response message (transaction authenticated via 3DS)**

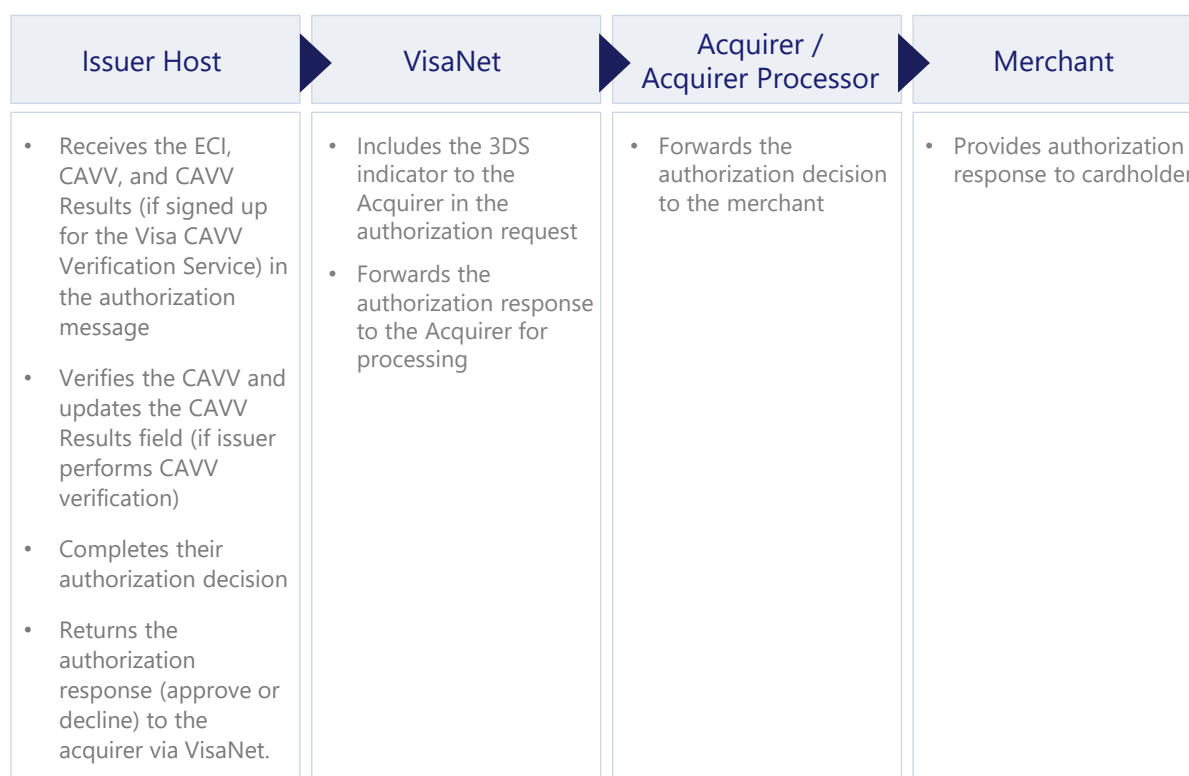


Table 3 summarizes the key relevant ECI values returned by 3DS. The format and role of the CAVV is summarized in more detail in Section 3.2.7.

**Table 3: ECI values**

ECI Value	Authentication Status	Liability
ECI 05	Cardholder authenticated by the Issuer	Issuer
ECI 06	Merchant attempted to authenticate the cardholder but either the cardholder or Issuer is not participating in 3DS or the Issuer's ACS is currently unavailable	Issuer
ECI 07	Payment authentication has not been performed	Acquirer

Table 4 summarizes the key relevant message fields in the authorization message flow.

It should be noted that some transaction status indicators must be flagged by Issuers and some by Acquirers. It is key that merchants use MIT indicators for MIT transactions and the correct MOTO information for MOTO transactions.

**Table 4: Summary of authorization fields and messages used to communicate SCA and authorization status**

Field	Set by	Function	Field Value/Indicator
F19	Acquirer	Populated with the Acquiring Institution Country Code allowing the Issuer to determine whether the transaction is in or out of scope of SCA	Acquiring Institution Country Code
F25	Acquirer	Point-of-Service Condition Code – required for CAVV processing which in addition can be used to indicate MOTO transactions	Existing values as defined in the Visa technical specification <sup>14</sup>
F34	Acquirer	<p>Allows Acquirer to indicate that authorization is being requested without the application of SCA because one of the following exemptions applies:</p> <ul style="list-style-type: none"> <li>• Trusted Beneficiary</li> <li>• Low Value</li> <li>• Secure Corporate Payments</li> <li>• Transaction Risk Analysis</li> </ul> <p>or that the transaction has been authenticated under the terms of the Visa Delegated Authentication Program allows Visa to indicate to Issuers that a transaction is an MIT out of scope of SCA</p> <p>Allows Acquirers to indicate that there is an outage in the acceptance environment and it is not possible to authenticate.</p>	<p>The following tags are used to carry the SCA exemption indicators in the new TLV Field 34 Dataset ID Hex 4A:</p> <ul style="list-style-type: none"> <li>• Tag 84 - Trusted Merchant Exemption Indicator. Possible values: <ul style="list-style-type: none"> <li>• <b>0</b> (Trusted merchant exemption not claimed/requested)</li> <li>• <b>1</b> (Trusted merchant exemption claimed/requested)</li> <li>• <b>2</b> (Trusted merchant exemption validated/honored)</li> <li>• <b>3</b> (Trusted merchant exemption failed validation/not honored)</li> </ul> </li> </ul> <p>NOTE: <i>If the trusted merchant exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely.</i></p> <ul style="list-style-type: none"> <li>• Tag 87 - Low Value Exemption Indicator Possible Values <ul style="list-style-type: none"> <li>• <b>0</b> (Low value exemption does not apply to the transaction)</li> <li>• <b>1</b> (Transaction exempt from SCA as the merchant/Acquirer has determined it to be a low value payment)</li> </ul> </li> </ul> <p>NOTE: <i>If the low value exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely.</i></p> <ul style="list-style-type: none"> <li>• Tag 88 - Secure Corporate Payment (SCP) Indicator Possible Values: <ul style="list-style-type: none"> <li>• <b>0</b> (SCA exemption does not apply to the transaction)</li> <li>• <b>1</b> (Transaction exempt from SCA as the merchant/Acquirer has determined it as a secure corporate payment)</li> </ul> </li> </ul> <p>NOTE: <i>If the SCP exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely.</i></p> <ul style="list-style-type: none"> <li>• Tag 89 - Transaction Risk Analysis (TRA) Exemption Indicator Possible Values:</li> </ul>

<sup>14</sup> For more details, refer to the *V.I.P. Base 1 Technical Specifications, Volume 1 & Volume 2*.

Field	Set by	Function	Field Value/Indicator
			<ul style="list-style-type: none"> <li>• <b>0</b> (Transaction risk analysis exemption not claimed/requested.)</li> <li>• <b>1</b> (Transaction risk analysis exemption claimed/requested.)</li> </ul> <p>NOTE: If the TRA exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely</p> <ul style="list-style-type: none"> <li>• Tag 8A - Tag indicates that the transaction is using Visa Delegated Authentication during authorization; also referred to as the Delegated Authentication indicator</li> </ul> <p>Possible Values:</p> <ul style="list-style-type: none"> <li>• <b>0</b> (Delegated authentication does not apply to the transaction)</li> <li>• <b>1</b> (Issuer has delegated SCA)</li> </ul> <p>NOTE: <i>If the delegated authentication does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely</i></p> <p>Apart from the exemption tags present in Dataset ID Hex 4A, two additional tags are present in Dataset ID Hex 02:</p> <ul style="list-style-type: none"> <li>• Initiating Party Indicator – Tag 80 This is used to indicate to the Issuer that this transaction was flagged as an MIT. This field cannot be populated by an Acquirer. Visa net will populate this value if the Acquirer has indicated the transaction is an MIT using the MIT Framework. Possible Values: • <b>1</b> (Populated by Visa if Acquirer indicated this transaction as Merchant Initiated)</li> <li>• Acceptance Outage Indicator – Tag 87 The indicator means that authentication was attempted for a transaction but there was an authentication outage in the authentication flow between the merchant, gateway 3-D Secure (3DS) server, and directory server, which means an authentication request was not possible and an authentication response could not be received. (This indicator cannot be used to indicate an outage in the Issuer processing domain, including agents acting on behalf of the Issuer). Possible Values: • <b>0</b> (No authentication outage) • <b>1</b> (Authentication outage) If there is no Authentication outage, the value of 0 is optional and the tag may be omitted entirely.</li> </ul> <p>In Dataset ID 01, there is Tag 86 called 'Authentication data'. This will include the 3-D Secure Protocol version number and is populated by Visa. Values:</p> <ul style="list-style-type: none"> <li>• <b>1.x.x</b> (3DS 1.x.x)</li> </ul>

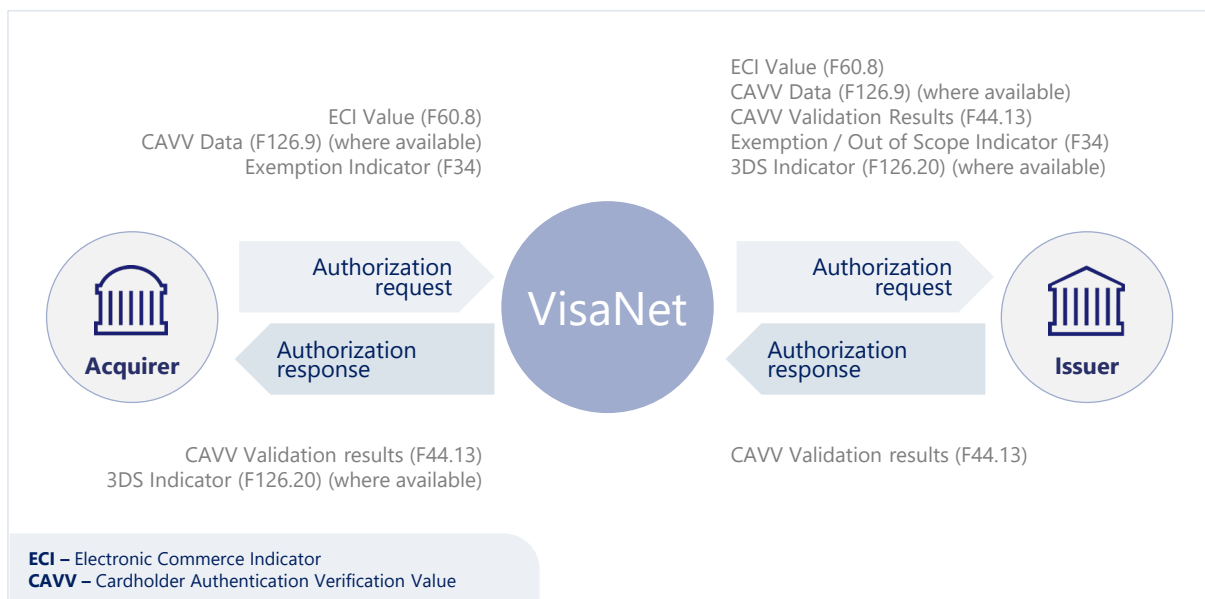


Field	Set by	Function	Field Value/Indicator
			<ul style="list-style-type: none"> <li>• <b>2.x.x</b> (EMV 3DS 2.x.x)</li> <li>• <b>2.2.x</b> (EMV 3DS 2.2.x)</li> <li>• <b>UNKNOWN</b> (Unknown 3DS protocol version number)</li> </ul>
F39	Issuer	Response to F34 exemption request indicating additional customer authentication required	Response code 1A – SCA Decline Code
F44.13	Acquirer	CAVV /TAVV Results Code	One-character code indicating classification of the CAVV / TAVV and the pass/fail result. For token transactions, if no CAVV, the TAVV result code can be populated here. If both are present, then the CAVV Result Code is in this field and the TAVV Result Code is in field 123
F60.8	Acquirer	Mail/Phone/Electronic Commerce and Payment Indicator indicating the ECI Value	Existing values as defined in the Visa technical specification <sup>14</sup>
F60.10	Acquirer	Indicates a transaction performed with an estimated amount	2 or 3
F62.2	Acquirer – when submitting an MIT (otherwise set by Visa on every single transaction)	<p>May be used by Acquirers to indicate a transaction is an MIT: Acquirers may indicate the Tran ID of the initial CIT (or in some instances of a previous MIT) associated with the current MIT in either F62.2 or F125. Visa forwards this information to Issuers only in F125</p> <p>The Tran ID seen by Issuers in F62.2 is that of the current MIT, as sent by Visa, and not that of the initial CIT</p>	This is a 16 digit value
F63.3	Acquirer	<p>Indicates if the transaction is an out of scope MIT of the following type:</p> <ul style="list-style-type: none"> <li>• Incremental</li> <li>• Delayed Charges</li> <li>• No Show</li> <li>• Resubmission</li> <li>• Reauthorization</li> </ul> <p>Indicates the transaction is deferred.</p>	<p>Values 3900 to 3904 indicate MITs</p> <p>Value 5206 indicates the transaction is deferred, i.e. that it could not be submitted at the time of the Transaction due to no connectivity, system issue or other limitations.</p>
F123	VisaNet	Contains additional data relating to a token transaction	Includes the TAVV Results Code in Dataset 67, tag 08.
F125	Acquirer	Acquirers may indicate the Tran ID of the initial CIT (or in some instances of a previous MIT) transaction associated with the current MIT in either F62.2 or F125. Visa forwards this information to Issuers only in F125	For Issuers in an MIT transaction, the Tran ID associated with the initial CIT (or in some limited instances the with a previous MIT) where agreement was set up (and SCA performed) see Section 3.9.2.1 for more details
F126.13	Acquirer	Used to indicate (with F125 or F62.2) if the transaction is a Recurring,	Value R, I or C

Field	Set by	Function	Field Value/Indicator
		Installments/Prepayment or Unscheduled Credential on File out of scope MIT	
F126.20	VisaNet	3DS Indicator: optional field that identifies the authentication method used by the Issuer ACS (e.g. Risk Based Authentication). For more details see below	Values 0 to F – see Table 5 in Section 3.2.6
F126.8	Acquirer	TAVV Data	If CAVV and TAVV are present, then TAVV Data is in this field. If only TAVV is present, then Acquirer can populate in this field of field 126.9
F126.9	Acquirer	CAVV / TAVV Data	Usage Field 3 supported for EMV 3DS If CAVV is present, this field contains the CAVV. For token transactions without a CAVV, the TAVV can optionally be delivered in this field

The function of each of these fields and the values/tags is described in more detail below.

**Figure 6: Main message flows for a simple e-commerce transaction**



### 3.2.3 VisaNet Field 34 & SCA decline code (Response Code 1A) in Field 39



Visa has implemented Field 34 to support PSD2 SCA requirements by indicating an Acquirer applied exemption. Additionally, an SCA decline code (Response Code 1A) in Field 39 is available to Issuers to indicate that the transaction cannot be approved until SCA is applied.

#### Requirement

Acquirers should specify only one SCA exemption indicator per authorization request.

If an Acquirer requests an exemption in the authentication process, it must be mirrored during authorization. The Acquirer is responsible for this monitoring activity and ensuring that the correct indicator is used throughout the authorization process.

Issuers are required to consider SCA exemption indicators and out of scope information when deciding whether or not to approve an authorization request.

Acquirers can use Field 34 to submit e-commerce transactions that may include one of the SCA exemption indicators in order to communicate to the Issuer why SCA was not performed on an e-commerce transaction. However, Acquirers should specify only one SCA exemption indicator per transaction message. In the event that the Acquirer specifies multiple SCA exemption indicators, V.I.P. will pass all the SCA exemption indicators available in the transaction to the Issuer, however this may have an adverse impact on Issuers' approval rates. Issuers are required to consider SCA exemption indicators and out of scope information when deciding whether or not to approve an authorization request.

The tags listed in Table 4 above, are used to carry the SCA exemption indicators in the Field 34 Dataset ID 4A. These tags are ISO specification compliant and are no longer Visa specific.

Field 34 Dataset ID 56 also supports the addition of optional supplemental data through two new tags. These carry the consumer device IP address and the Visa Consumer Authentication Service (VCAS) score, for Issuers using VCAS. This supplementary information aims to help Issuers improve their approval rates.

Issuers and Acquirers in Europe are mandated to support all SCA tags in Field 34 Dataset Hex4A. The Tags in Dataset 02, i.e. the MIT Tag in Tag 80 is optional if Issuers choose to recognise MITs via the MIT framework. Additionally the Acceptance Outage Indicator in Tag 87 is also optional as of the upcoming release (Oct 2020, Jan 2021). The right to apply and/or accept the exemptions indicated in Field 34 remains that of the Acquirer and Issuer, and all parties must be technically capable of sending and receiving these fields.

Issuers must complete VisaNet Certification Management Service (VCMS) certification before the field is activated.

Table 22 in section 1094.4 provides a simple summary of the indicators for the key exemptions along with the liability for fraud related chargebacks.

#### 3.2.3.1 Impact for Acquirers

Acquirers in the Europe region must be able to:

1. Support Field 34—Electronic Commerce Data, Dataset ID 4A—Supplemental Data in TLV format with tags to indicate whether an e-commerce transaction is exempt from the PSD2/RTS SCA mandate

2. Receive the SCA decline code in existing Field 39

SCA decline code will be converted to 05 (Do not honor) in Field 39 if the non-EEA Acquirer's parameter is not activated in VisaNet to receive the SCA decline code.

Certification is required for Acquirers to support TLV Field 34, which contains the new SCA exemption indicators in Dataset ID 4A. Additional certification is not required for Acquirers to receive the SCA decline code in existing Field 39.

### 3.2.3.2 Impact for Issuers



Issuers in the Europe region must:

1. Be able to receive TLV Field 34—Electronic Commerce Data
2. Use the SCA decline code when a transaction has been declined due to the absence of SCA
3. Not use the SCA decline code for a transaction that is out of scope of SCA

Issuers may respond with the SCA decline code for both e-commerce and card present contactless point of sale (POS) transactions.

Issuers that choose to receive the supplemental data must be able to receive the new Field 34 - Electronic Commerce Data, Dataset ID 56 - Supplemental Data in TLV format with new tags and must be aware of new processing rules to support the new supplemental data.

Issuers must not use SCA decline code for all transactions out of scope of SCA or not requiring SCA.

transactions that are deemed out of scope of SCA from a regulatory perspective, specifically:

- a. MOTO transactions
- b. Merchant Initiated Transactions
- c. Transactions performed with an anonymous payment instrument (e.g. an anonymous prepaid card)
- d. Transactions from a merchant acquired by an Acquirer located outside the EEA (one-leg-out transactions). These merchants are asked to perform SCA 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

Other transactions that do not contain a valid CAVV where SCA is not required, specifically:

- a. Zero value authorization/account verification requests
- b. Original Credit Transactions
- c. Refunds

For more information on Visa Rules governing the use of the SCA decline code please see *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements*. For information on identification of transactions that do not require SCA see sections 3.2.9 and 4.2.4.2.

### 3.2.3.3 Use of SCA decline codes in cross border transactions

From the relevant regulatory enforcement dates for e-commerce, Issuers within the EEA and the UK will be required to request that any transaction submitted without SCA or without a correct out of scope or exemption indicator is responded to with a request to resubmit with SCA or the transaction will be declined. Under managed migration programs being implemented in some markets the so called "soft decline" (SCA decline code) will be applied progressively by Issuers ahead of the enforcement date.

As enforcement dates may vary between markets, notably between the EEA and the UK, there will be a period when there is a heightened risk of declines if EEA Issuers respond to cross border transactions at, for example, UK acquired merchants with an SCA decline code while UK merchants are still unable to respond to the code and submit the transaction for authentication. This may result in merchants that are unable to respond losing transactions.

Subject to any further developments, the UK could become a third country for the purposes of PSD2 from 1 January 2021. The UK currently plans to enforce equivalent requirements to SCA for e-commerce in the UK from 14 September 2021, but until this point the UK may be considered 'one-leg-out'.

Therefore, during this time, relevant PSPs may need to apply SCA on a best efforts basis which may in some circumstances mean Issuers choose not to decline transactions without SCA. The Issuer should make their own approval decision based on risk, customer experience and liability considerations. On this basis:

- EEA Issuers should not use SCA decline codes for UK acquired transactions during the period 01 January to 14 September 2021. If an Issuer decides that they do not want to approve the transaction, they should decline with another appropriate response code.
- EEA and UK Issuers can and should use SCA decline codes for EEA/UK cross border transactions from 14 September 2021

For guidance, on the recognition of one-leg-out transactions please see sections 2.3.2, 2.3.3 and 3.2.9.

### 3.2.4 MIT out of scope indicator for Issuers in Field 34



Visa has introduced a new indicator<sup>15</sup> to help Issuers to identify a transaction that is an MIT and out of scope of SCA. The indicator is a value of "1" in Field 34 (Tag 80, Dataset ID 02) i.e. the same field Issuers use to check for exemptions to SCA.

---

<sup>15</sup> See *Article 9.1.4 Changes to Identify Merchant-Initiated Transaction as Out of Scope for Strong Customer Authentication, Oct 19* for more details.

Visa will automatically populate the value of "1" in TLV Field F34, Tag 80, Dataset ID 02 when receiving a transaction indicated as an MIT by the Acquirer using the MIT Framework. Refer to section 3.9 for more details.

An Issuer activated to receive F34 will automatically receive this value when the Acquirer has indicated the transaction as merchant-initiated using the MIT Framework.

This enables Issuers to recognize a transaction as an out of scope MIT by simply looking for the value of "1" in that tag. Issuers may alternatively decide to recognize an MIT out of scope by looking at the indicators from the MIT Framework. See section 3.9 for more details.

An Issuer must not use an SCA decline code in a transaction legitimately indicated as an MIT as the cardholder is not available to be authenticated.

An Acquirer cannot use Field 34, Tag 80, Dataset ID 02 to indicate an MIT out of scope.

### 3.2.5 New acceptance environment outage indicator in Field 34



Effective 22 January 2021, Visa is introducing a new 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 acceptance environment.

More specifically, the indicator means that authentication was attempted for a transaction but there was an authentication outage in the authentication flow between the merchant, gateway 3-D Secure (3DS) server, and Directory Server, which means an authentication request was not possible and an authentication response could not be received (this indicator should not be used to indicate an outage in the Issuer processing domain, including agents acting on behalf of the Issuer).

#### 3.2.5.1 Issuer impact



Using this indicator is optional for Acquirers. Receiving this field is mandated for Issuers from the April 2021 Business release. Acting on this indicator is however optional for Issuers. Both Acquirers and Issuers 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. 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.

Approving transactions with this flag and without authentication is at the Issuer's discretion. It is recommended that in deciding their authorization policies with respect to this indicator, Issuers:

- Consider regulatory requirements balanced with the intent to support resilience/business continuity/cardholder experience. Issuers could for example decide to support the indicator every time it is sent or could decide to authorize flagged transactions only when the outage is major/longer than unusual. Each Issuer needs to determine its own policies

- Perform risk based analysis on each transaction and decline if the transaction is high risk
- Ensure that reasons to decline other than lack of authentication are considered first as usual (e.g. declines for insufficient funds, block card or similar that would inform the merchant there is no opportunity for an approval)

Considering that authentication is not available due to an outage, European Issuers are recommended to carefully consider whether use of an SCA decline code is appropriate. An SCA decline code may indicate to the merchant that if the option is available to resubmit with authentication once the 3DS environment is accessible, the Issuer may reconsider the response if authentication is provided. Issuers should note however that authentication may not be possible if the customer is no longer available.

### 3.2.5.2 Acquirer impact



The use of the indicator is optional for Acquirers. Acquirers need to consider regulatory requirements and resilience imperatives before deciding to use this indicator. Acquirers must be aware of additional conditions that will apply for their merchants to be permitted to use this indicator, including Acquirer monitoring requirements<sup>16</sup>.

### 3.2.6 Deferred authorization indicator in F63.3



This indicator (value of 5206 in Field 63.3) indicates that a transaction was deferred, i.e. it could not be submitted because there was no connection available or there was another system issue at the time of authorization. This prevented authorization from occurring at the time of the transaction, which also meant there was no ability to authenticate. Merchants should collect the transaction information and send a deferred authorization request at the earliest possible opportunity. Such a connectivity issue may occur for example when airlines or train operators make sales in transit.

#### 3.2.6.1 Issuer impact



Recognizing and acting on this indicator is optional for Issuers. Issuers should consider their regulatory obligations before deciding whether to use this indicator. Transactions containing this indicator do not represent transactions that can be considered exempt or out of scope of the SCA regulation, but the presence of this indicator enables Issuers to understand that this is a transaction where authentication could not be performed due to lack of connectivity at the time of the transaction. The transaction can be submitted by the merchant when connectivity is restored, which may be when the customer is no longer available to authenticate and the goods and services may have already been provided.

#### 3.2.6.1 Acquirer impact



Merchants are required to include this indicator on all deferred authorization requests from 16 April 2021. Merchants are recommended to use the indicator as soon as possible in any

<sup>16</sup> These conditions will be documented in *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements*.

deferred authorization so that Issuers can recognise that the transaction has been deferred due to lack of connectivity.

This may minimise, but not eliminate cases where the Issuer responds to an authorization request with an SCA decline code as approving transactions with this flag and without authentication is at the Issuer's discretion. To optimise the chance of approval, merchants should consider requesting an exemption if one is applicable to that transaction.

### 3.2.6 The new VisaNet 3DS Indicator Field 126.20



Visa has included a new optional field in an authorization – 3DS Indicator (Field 126.20) – to identify the authentication method used by the Issuer's ACS to authenticate the cardholder (e.g. risk-based authentication or OTP).

This field provides Issuers with more visibility into the authentication process during authorization for use in decisioning.

The 3DS Indicator value is derived from Position 2 of the CAVV present in Field 126.9.

Issuer host systems can now choose to receive the 3DS Indicator (Field 126.20). Issuers planning to utilize the new 3DS Indicator Field 126.20 will need to take account of the following:

- A new CAVV format is required, which includes the authentication result for all EMV 3DS transactions
- The updated CAVV format can be used with 1.0 transactions, but the authentication method will not be provided
- Issuers that want to receive F126.20 must complete VisaNet Certification Management Service (VCMS) certification before the field is activated

The field is optional, so there is no impact on Issuers that do not wish to receive this field.

#### Best Practice

Issuers are strongly encouraged to use Field 126.20 as it provides valuable information about the authentication to help better authorization decisioning.

Field values are shown in Table 5 below.



**Table 5: The values for Field 126.20**

3DS Indicator Value	3DS Description
0	3DS 1.0.2 or prior all authentication methods
1	Challenge flow using Static Passcode
2	Challenge flow using OTP via SMS method
3	Challenge flow using OTP via key fob or card reader method
4	Challenge flow using OTP via App method
5	Challenge flow using OTP via any other method
6	Challenge flow using KBA method
7	Challenge flow using OOB with Biometric method
8	Challenge flow using OOB with App login method
9	Challenge flow using OOB with any other method
A	Challenge flow using any other authentication method
B	Unrecognized authentication method
C	Push Confirmation
D	Frictionless flow, RBA Review
E	Attempts Server responding
F	Frictionless flow, RBA
G	Issuer defined ACS-specific authentication method 1 <sup>17</sup>
H	Issuer defined ACS-specific authentication method 2 <sup>17</sup>
I	Issuer defined ACS-specific authentication method 3 <sup>17</sup>
J	Issuer defined ACS-specific authentication method 4 <sup>17</sup>
K	Issuer defined ACS-specific authentication method 5 <sup>17</sup>

### 3.2.7 CAVV / TAVV Support and Fields 126.8, 126.9 and 44.13



The CAVV is a unique cryptogram created for each 3DS authenticated transaction. It provides proof that cardholder authentication occurred or that the merchant attempted authentication. Visa requires Acquirers to include CAVV data for all 3DS authenticated transactions (ECI 05 and ECI 06). Any ECI 05 or ECI 06 transactions without a CAVV will be downgraded to ECI 07 and the Acquirer will no longer benefit from fraud liability protection.

<sup>17</sup> CAVV v7 only.

The use of CAVV helps secure the integrity of 3DS transactions, enables end-to-end transaction traceability and further streamlines the dispute/chargeback process.

### 3.2.7.1 Use of the CAVV

The CAVV is generated and populated as follows:

- The CAVV is generated by the Issuer’s ACS when a successful authentication is completed, or by Visa when the Visa Attempts Server when it stands in for the Issuer’s ACS (ECI 06)
- Each step in the authentication process is validated by the Issuer or the Issuer’s ACS on their behalf and should the validation fail at any point, a CAVV would not be generated
- Measures should be in place to ensure the CAVV cannot be compromised
- The CAVV is a cryptographic representation of the amount and payee as agreed by the payer and as such may not necessarily include the actual raw data (CAVV version 7 only).
- Visa’s authentication code is dynamically linked to the amount and the payee
- The merchant populates F126.9 with the CAVV which is then validated by the Issuer (or Visa where CAVV keys are provided) during authorization

Three versions of the Visa CAVV are available. Visa considers that all versions support the PSD2 dynamic linking requirement however Visa expects all Issuers to adopt version 7 which provides enhanced dynamic linking capabilities and supports EMV 3DS. As of 17 April 2021 European Issuers are required to use CAVVv7 for EMV 3DS transactions<sup>18</sup>.

Table 6 summarizes the key characteristics of each Version:

**Table 6: CAVV characteristics**

Characteristics Supported	CAVV Version 0	CAVV Version 1	CAVV Version 7
3DS Version	3DS 1.0 and EMV 3DS <sup>19</sup>	3DS 1.0 only	3DS 1.0 and EMV 3DS
Merchant Name	No	No	Yes <sup>20</sup>
Amount	No	No	Yes
Linking	Yes (reactive)	Yes (reactive)	Yes (real time)

For more information of the CAVV creation, verification and use in authorization please refer to *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.

<sup>18</sup> See VBN AI10570 “Extended Support for CAVV Usage 3, Version 0 in Europe” for further information.

<sup>19</sup> See VBN AI10570 “Extended Support for CAVV Usage 3, Version 0 in Europe” for information on support for CAVVv0 and EMV 3DS.

<sup>20</sup> A hashed version of the authentication merchant name is provided in version 7 of the cryptogram.

Issuers can use the CAVV to link to the authentication message, thus meeting the dynamic linking requirement. Issuers can check that the amount submitted for authorization does not exceed the amount authenticated, as required under dynamic linking, by checking the Authentication Amount in the CAVV. Note that Authentication Amount is only available in CAVV U3 V7. For more details on how to do this please refer to *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.

Issuers may additionally choose to:

- Investigate specific transactions such customer disputed transactions
- Validate the (hashed) merchant name and transaction amount from the authentication message in real time.

Merchants must ensure that the 3DS authentication request is accurately populated with the following information:

- Total transaction amount
- Merchant descriptor name<sup>21</sup> (where required)
- 3DS requestor ID

Visa requests that until 1 September 2022 Issuers allow a CAVV to be used up to five times. Note that if a CAVV is used in a transaction that is declined, this instance does not count as one of the five allowed instances<sup>22</sup>.

### 3.2.7.2 TAVV Data in Field 126.8

Field 126.8 allows Acquirers to:

- Send the TAVV data received from VTS in the authorization and full financial request messages with the ECI value

Acquirers must be capable of sending the TAVV data as described above for token based 3DS transactions.

Visa also strongly recommends that Acquirers send TAVV Data in Field 126.8 when this is the only cryptogram data sent in token transactions without 3DS. However, Visa will continue to process the token transaction if TAVV was sent in Field 126.9, Usage 3.

For token transactions that go straight to authorization without first performing 3DS, Field 126.9 can optionally be populated with the TAVV.

### 3.2.7.3 CAVV / TAVV Data in Field 126.9

Field 126.9 allows Acquirers to:

---

<sup>21</sup> For more information on populating the merchant name when the party requesting authentication is not the merchant that will request authorization see Section 4.7.3.7. Detailed guidance on dealing with merchant naming in travel agent booking use cases is given in the supplement to this guide: *Implementing Strong Customer Authentication (SCA) for Travel & Hospitality*.

<sup>22</sup> Visa has temporarily amended its rules to allow the reuse of the CAVV up to five times, until 1 September 2022, for split shipment scenarios and scenarios where transactions are associated with bookings via travel agencies. The previous rule expired on 1 September 2020 and Visa has now extended the expiration date to 1 September 2022. For more information please see VBN Article ID: A110292 *Update to CAVV—Exceptions to Reuse in Europe 20 August 2020*.

- Include the CAVV data in the authorization and full financial request messages with the ECI value

Acquirers must be capable of sending the CAVV data as described above. If an Acquirer does not include CAVV data in field 126.9 for an ECI 05 or ECI 06 transaction, the ECI value will be downgraded to ECI 07 (non-authenticated).

For token transactions that go straight to authorization without first performing 3DS, Field 126.9 can optionally be populated with the TAVV, however, Visa strongly recommends that Acquirers send TAVV Data in Field 126.8.

### 3.2.7.4 Field 44.13 CAVV Results Code

Field 44.13—CAVV Results Code contains a one-character code that indicates the following:

- The classification of the transaction (either an authentication transaction where the Issuer ACS has created the CAVV or an attempts transaction where the Visa Attempts Server has created the CAVV)
- For an authentication transaction, where the Issuer ACS has created the CAVV
- For an attempts transaction, where the Visa Attempts Server has created the CAVV
- The CAVV verification result:
  - CAVV verification passed
  - CAVV verification failed

For token transactions that go straight to authorization without first performing 3DS, Field 44.13 can optionally be populated with the TAVV results code, but only if the Issuer does not support field 123.

CAVV Results code values and descriptions are included in the *VisaNet Business Enhancements Global Technical Letter and Implementation Guide October 2018 Version 3.0 (Major Release) and January 2019 Version 2.0 (Minor Release) – effective 6 September 2018*.

### 3.2.7.5 Use of the CAVV in account verification

To support the account verification transaction where SCA is performed, effective 16 October 2020, all Acquirers and Issuers in Europe will be required by Visa to receive the CAVV Results Code when it is present in account verification transactions. Clients should refer to Article 9.1.2—Mandate to Support CAVV Results Code Field in Account Verification Transactions in the Europe Region in the *October 2020 and January 2021 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 18 June 2020* for more information on the change and its processing impact. For more information on account verification use cases please refer to section 4.7.3.2.

Issuers and Acquirers will not need to raise an implementation project or request an activation for this feature. All Issuers and Acquirers will be mass-enrolled during the October 2020 VisaNet Business Enhancement release.

Issuers and Acquirers that would like to enable this feature before the October VisaNet Business Enhancements release can do so as part of the July 2020<sup>23</sup> Business Enhancement release. Visa will allow Issuers and Acquirers to 'opt in' to receive the CAVV Results Code.

For more information of the CAVV creation, verification and use in authorization please also refer to *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide*.

### 3.2.8 Acquirer support of ECI and CAVV Data



Acquirers that support e-commerce, or application-based e-commerce transactions for PANs or tokens must be prepared to support the following:

- ECI 07 in existing Field 60.8—Mail/Phone/Electronic Commerce and Payments Indicator in authorization request messages
- ECI 07 in existing Field 63.6—Chargeback Reduction/BASE II Flags, position 4, MOTO/ECI Indicator in full financial request messages
- CAVV data in existing Field 126.9—CAVV Data, Usage 3: 3-D Secure CAVV, Revised Format in authorization and full financial request messages
- ECI 07 in BASE II Draft Data

Issuers will continue to have the option to receive existing CAVV and ECI fields to support CAVV processing.

### 3.2.9 Identifying Out of Scope & other transactions not requiring SCA



The following transaction types are out of scope of SCA

- Mail Order/Telephone Order (MOTO)
- Merchant Initiated Transactions (MITs)
- One-Leg-Out (OLO) transactions<sup>24</sup>
- Anonymous transactions

Out of scope transactions are identified as summarized in Table 7 below.

<sup>23</sup> Refer to Article 4.9—Changes to Support CAVV Data in Account Verification Transactions in the *April 2020 and July 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 12 March 2020*.

<sup>24</sup> Although One-Leg-Out transactions are out of scope, Acquirers and merchants are reminded that SCA should still be performed on a best effort basis.

**Table 7: Out of scope of SCA transaction indicators**

Out of Scope Transaction Type	Indicators
MOTO	<p>Mail order and telephone order (MOTO) transactions are out of scope of SCA and are indicated in the Visa processing system by a value of:</p> <ul style="list-style-type: none"> <li>• 08 in Field 25, and/or</li> <li>• 01 or 04 in Field 60.8</li> </ul>
Merchant Initiated Transactions (MITs)	<p>Merchant Initiated Transactions identified by Acquirers through the use of the Visa MIT Framework and by Issuers either by the use of the MIT Framework or by the MIT out of scope indicator (value 1) in Tag 80, dataset 2 of Field 34<sup>25</sup></p>
One-Leg-Out (OLO)	<p>In the Visa processing system, these transactions are recognized by:</p> <ul style="list-style-type: none"> <li>• An Issuer BIN outside of the EEA or UK<sup>26</sup>, or</li> <li>• An Acquirer location outside of the EEA or UK (Field 19 – Acquiring Institution Country Code)</li> </ul> <p>In EMV 3DS these transactions can be recognized by</p> <ul style="list-style-type: none"> <li>• The Acquiring Institution Country Code (ACC) indicator in the EMV 3DS ACC extension, which is available for EMV 3DS 2.1 and 2.2</li> </ul> <p>Note that in these cases, SCA should still be applied on a ‘best effort’ basis so SCA may be present. For more information on one-leg-out use cases and application of best efforts please see section 2.3.2</p>
Anonymous	<p>Transactions performed with anonymous cards<sup>27</sup> are out of scope of SCA; however, they cannot be recognized as such by merchants. In this case, the following approaches are possible for merchants:</p> <p><b>Option 1</b> - They can proceed to authentication - in which case,</p> <ul style="list-style-type: none"> <li>• When the card is not enrolled and not participating in 3DS, the response, in EMV 3DS, will be an ARES = N with an ECI 07 and “Not Authenticated/Account Not Verified” message and a transaction status response code will be sent with a Transaction Status Reason Code 87 “Transaction is excluded from Attempts Processing e.g. non-reloadable, TRA, etc.”</li> </ul>

<sup>25</sup> See Section 3.9 for more details. Note that in addition to transactions not initiated by the payer (and which are therefore out of scope), the MIT field will also flag transactions which are not out of scope but where SCA has already been performed or an exemption was applied before the transaction was executed – only for specific cases outlined in Section 3.9.

<sup>26</sup> Note: While the requirement to apply PSD2 SCA currently applies in the UK, current uncertainty over the status of PSD2 in any trade agreement between the UK and EU and the divergence in enforcement dates between the UK and EEA means there may be a period from 1 January 2021 when cross border transactions between EEA states and UK may be considered One-Leg-Out. For more information, please see section 2.3.3.

<sup>27</sup> In the Visa system, these can include non-reloadable prepaid cards on which no KYC has been done and thus where the Issuer cannot authenticate the identity of the cardholder. The card is not enrolled in 3DS. The fact that no KYC has been done and/or that it is a non-reloadable prepaid card will not necessarily mean the card is anonymous in all cases.

	<ul style="list-style-type: none"> <li>When the card is enrolled but not participating in 3DS, the response will be an ARES = N with an ECI 07 and a Transaction Status Reason code of the Issuer's choosing conveying the card cannot be authenticated</li> </ul> <p>Upon receiving such responses, the card may be an anonymous one so merchants should send transaction to authorization</p> <p><b>Option 2</b> - They can proceed direct to authorization in which case Issuers are being asked to recognize BINs/account ranges for out of scope cards and should not request SCA on anonymous cards</p>
--	---

Visa considers that SCA may not be required to be performed by the cardholder for the following additional transactions summarized in Table 8:

**Table 8: Identification of additional transactions not requiring SCA by the cardholder**

Transaction Type	Indicators
OCTs & refunds	<p>Original Credit Transactions (OCTs) and refunds do not require SCA to be performed by the recipient of the funds (i.e. the cardholder). Therefore, an Issuer may not use the SCA decline code in response to authorization requests properly identified as OCTs or refunds.</p> <ul style="list-style-type: none"> <li>Issuers can identify an OCT by checking for processing code value of 26 in Field 3.1. For more information, refer to Section 4.9. Issuers can identify a refund transaction by value 20 in Field 3.1 (if processed via authorization – most refunds are processed via clearing only).</li> </ul>
Zero value authorization/account verification requests	<p>Transaction where amount is zero. An Issuer will not be able to tell which of these transactions requires SCA (some legitimately do not). Issuers should refer to section 4.7.3.2 to recognize scenarios where they should/should not request SCA when the transaction is of zero value.</p>

### 3.2.9.1 Recognition of out of scope transactions - Acquirer impact



- If a payment transaction is out of scope of SCA, then the merchant / Acquirer must submit an authorization request ensuring that appropriate information is present that allows the Issuer to recognize that the transaction is out of scope, for example, by including relevant MIT indicators, or properly flagging as MOTO as described in the above table. Transactions that are not correctly flagged are at risk of being declined by Issuers. For example:
  - For MITs, this means supporting the MIT Framework for both PAN and token transactions
  - PAN key entered transactions submitted without any MOTO or MIT indicators(s) may not be recognized by Issuers as MOTO or MIT out of scope transactions.
  - Transactions that are key entered into a PoS system in order to complete a transaction associated with an indirect sales travel booking may often be MITs, subject to authentication being performed by the third party agent at the time of booking, to create the MIT mandate. The ability to flag MITs may require upgrading of and additional integration between PoS and booking systems used by booking

agents, intermediaries and merchants in order to pass the required authentication data. An interim solution allows these transactions to be flagged as MOTO as long as authentication has been applied at the time of booking (which is required unless the transaction qualifies for the secure corporate payments exemption) and other relevant requirements are met.<sup>28</sup> 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.

- MIT and MOTO indicators (with the exception set out above) can only be used for legitimate MOTO and MIT transactions.
2. Transactions that are acquired across most of the EEA from 1 January 2021 (and currently planned in the UK from 14 September 2021) are considered in scope, even if the merchant is outside the EEA and the UK. In this case, Acquirers should work with their merchants to ensure that SCA can be applied.
  3. Where the Acquirer is inside the EEA from 1 January 2021 (subject to any local variations, or from 14 September 2021 in the UK under current plans) but the Issuer is outside (one-leg-in), SCA should be applied on a best effort basis and Acquirers are recommended to send transactions for SCA, for example by submitting the transaction via 3DS, where this is supported by the non-EEA Issuer. Merchants can identify whether Issuers support 3DS and which version is supported through their gateway or 3DS server provider<sup>29</sup>.
  4. Acquirers are reminded to ensure that F19 is populated with the correct Acquiring Institution Country Code in the authorization message. If the Acquiring Institution Country Code is not present or is incorrect, the Issuer will not be able to determine whether or not SCA is required and may decline the transaction.
  5. Acquirers should note that the EMV 3DS ACC extension should not directly impact merchants and does not require any changes. The ACC will be populated by Visa upon receipt of the acquiring BIN in 3DS.

### 3.2.9.2 Recognition of out of scope transactions Issuer impact



Issuers in the Europe region must:

1. Be able to recognize every type of out of scope transaction. For MITs, they can do so using either the Visa MIT Framework or using the new MIT out of scope indicator in F34.

---

<sup>28</sup> Refer to VBN 10295 *Preparing Travel and Hospitality Merchants for SCA Compliance on Indirect Sales Transactions* for more details.

<sup>29</sup> For more information on identifying whether Issuers support 3DS and which version they support, see section 3.3.14.



- In the case that an Issuer selects to recognize MITs using the Visa MIT Framework, they must be able to receive the original Transaction ID in Field 125 if they do not already receive it (currently optional).<sup>30</sup>
2. Not use an SCA decline code, or equivalent, for authorization requests for transactions deemed out of scope from a regulatory perspective, or which does not otherwise require SCA as specified in Table 8 specifically when a merchant is not able to obtain SCA for MITs, MOTO, one-leg-out, or transactions performed with anonymous cards.<sup>31</sup> When Issuers receive a transaction without SCA they must always check the BIN before deciding whether to decline, in order to determine whether the card is anonymous.
  3. Identify transactions acquired outside the EEA and the UK through the Acquiring Institution Country Code in F19 of the authorization request, not by the merchant country code (Field 43).
  4. Recognize both indicator options identified in Table 7 above to ensure recognition of all MOTO transactions as merchants use either option.
  5. Issuers and their ACS vendors are impacted by the introduction of the EMV 3DS ACC extension. Issuers should work with their ACS vendors to ensure that this new data element is supported and implement appropriate processing rules.
  6. In the case of a one-leg-out transaction, if the EEA/UK<sup>32</sup> Issuer receives a request for authentication from a non-EEA/UK acquired merchant, they should decide whether to approve, apply SCA (where possible) or decline the transaction in line with the best efforts requirement, and considering the risk, customer experience and liability implications.

### 3.3 3-D Secure



This section provides a brief summary of the key features of 3-D Secure (3DS). More details and the full specifications are available from EMVCo at <https://www.emvco.com/emv-technologies/3d-secure>.

3DS is the industry standard solution adopted by card schemes, Issuers and Acquirers to enable the application of SCA. Merchants must support 3DS to facilitate the application of SCA which is required under PSD2. Visa rules do not preclude Issuers and Acquirers agreeing alternative means of performing SCA.

3-D Secure 2.0 (referred to in this guide as EMV 3DS, but also known as 3DS 2.0) is the new global specification for card payment security developed by EMVCo. It is designed to deliver frictionless payment authentication across a range of devices, including mobile handsets. Unlike previous versions of 3DS, it allows for more seamless integration with merchants' e-commerce customer experiences.

<sup>30</sup> For more information on the reception and use of the original Transaction ID please refer to Section 3.9.2.1.

<sup>31</sup> For more information please refer to: *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – Europe Region: Visa Supplemental Requirements for the European Economic Area*.

<sup>32</sup> Applies to the UK from 14 September 2021 under current enforcement plans.

Two versions of the EMV specification have so far been released. Version 2.1 (EMV 3DS 2.1) was released in October 2017 and went live Q4 2018. Version 2.2 (EMV 3DS 2.2) was released December 2018 and went live Q4 2019.

3-D Secure is used both for authenticating payment transactions and verifying the identity of the cardholder when the cardholder is setting up an arrangement for one or a series of Merchant Initiated Transactions.

Visa has adopted the brand name “Visa Secure” for Visa 3-D Secure in consumer branding and communications. For simplicity this guide just refers to 3-D Secure or 3DS.

Information about Visa’s 3-D Secure program can be found on the Visa Technology Partner site <https://technologypartner.visa.com/Library/3DSecure2.aspx>.

### 3.3.1 The benefits of EMV 3DS



EMV 3DS is a fundamental upgrade of the global standard for card-based e-commerce transaction authentication. The benefits it brings include:

- Use of Risk Based Authentication, utilizing a significantly increased number of transaction and customer data elements to securely authenticate the majority of transactions, without the need for additional customer friction
- Full compatibility with mobile and native app environments allowing mobile in-app, as well as mobile and computer browser transactions to be authenticated through a seamless user experience, even when SCA is required
- Integration with the merchant checkout user experience, including merchant branding options to further support a seamless customer journey
- Supports the SCA required request required when authenticating a new MIT agreement or responding to an SCA decline code

### 3.3.2 EMV 3DS implementation requirements & timescales



#### 3.3.2.1 The requirement to adopt EMV 3DS 2.2

EMV 3DS 2.2 provides further functionality which underpins the move to biometrics, the ability to take advantage of SCA exemptions and accommodates the delivery of a cryptogram in complex merchant use cases such as travel.

Enablement of EMV 3DS 2.2 across the ecosystem is an important step in effectively supporting the application of SCA and its exemptions. Visa recognizes that all parties are moving at pace to implement the new 3DS versions. To help further those efforts, Visa has implemented a technology roadmap to help ensure smooth industry-wide deployment of EMV 3DS.

## Best Practice

Merchants and Issuers are advised to adopt EMV 3DS 2.2 as early as possible in order to effectively support the application of PSD2 SCA and its exemptions. Merchants and Issuers should consult with their 3DS server and SDK vendors and ACS providers respectively on the timescales for implementation of EMV 3DS 2.2

### 3.3.2.2 EMV 3DS activation Issuer implementation dates

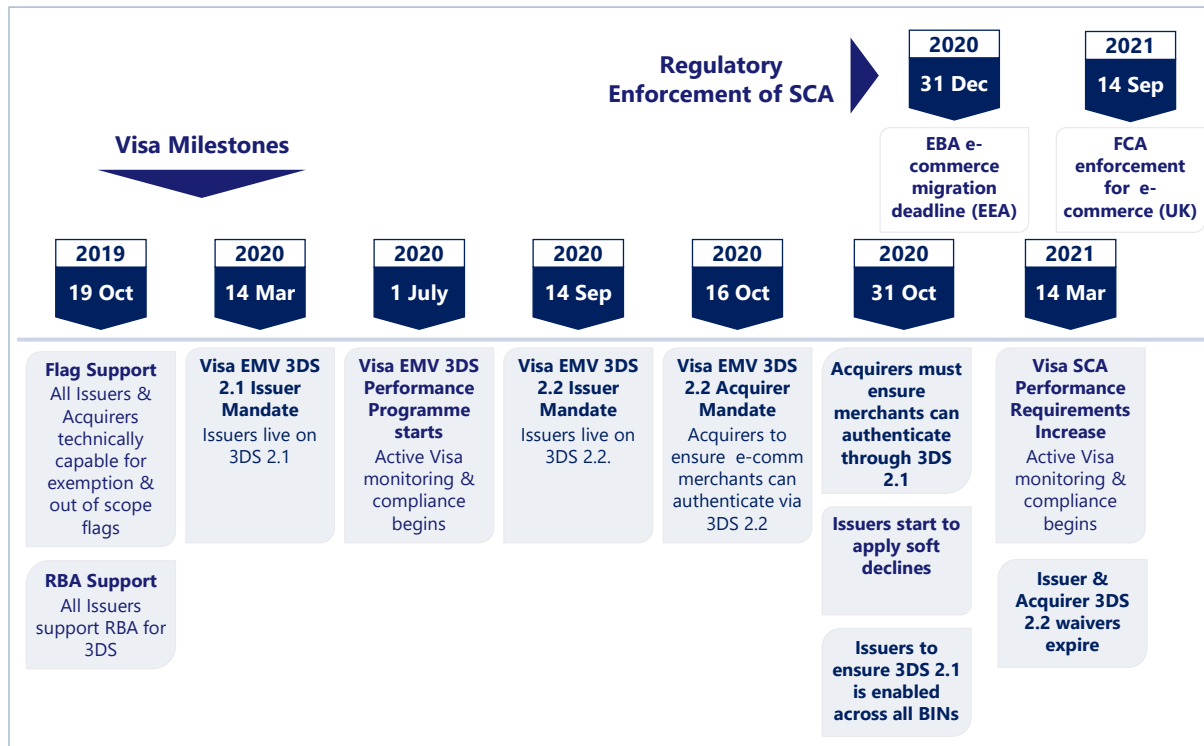
Visa Issuers have been required to support EMV 3DS 2.1 since 14 March 2020 and to support EMV 3DS 2.2 from 14 Sept 2020. Acquirers have been required to support EMV 3DS 2.2 from 16 October 2020.

Visa recognizes the importance of upgrading to EMV 3DS 2.2, but also understands the challenges that Issuers are facing in the current environment, and is offering a waiver on the EMV 3DS 2.2 mandate to all Issuers until 14 March 2021. This waiver is conditional on Issuers ensuring that EMV 3DS 2.1 has been enabled across all relevant issuing Bank Identification Numbers (BINs) by the end of October 2020.

### 3.3.3 Visa roadmap for EMV 3DS implementation

Visa has implemented a technology roadmap to help ensure smooth industry-wide deployment of EMV 3DS. This roadmap is summarized in Figure 7 below.

**Figure 7: Visa 3DS implementation roadmap**



### 3.3.4 3DS version feature comparison

The following Table 9 provides a comparison of the main features of 3DS 1.0, EMV 3DS 2.1 and EMV 3DS 2.2.

**Table 9: 3DS version notable feature comparison**

Notable Features	3DS 1.0	3DS 2.1	3DS 2.2
Capable of providing two factor authentication (2FA – static data, OTP)	Y	Y	Y
Dynamic linking - CAVV generated links authentication to the payment	Y <sup>33</sup>	Y	Y
Basic Issuer TRA (provided by the Issuer ACS)	Y	Y	Y
Mobile banking app integration	N	Y	Y
Biometric authentication	N	Y	Y
<i>Real time</i> Dynamic linking + - CAVV includes merchant name and amount	N	Y	Y
Mobile Device Compatibility	Basic	Y	Y
• Native	N	Y	Y
• HTML	Y	Y	Y
3RI			
• Non-Payment authentication	N	Y	Y
• Payment authentication with ability to obtain, refresh and regenerate CAVV	N	Y <sup>34</sup>	Y
• Decoupled authentication	N	N	Y
Decoupled authentication <sup>35</sup>	N	N	Y
Acquirer Exemption indicators			
• TRA performed prior to authentication	N	N	Y
• Trusted beneficiaries (whitelisting)	N	N	Y
Merchant/Acquirer request for SCA to be applied	N	Y	Y

<sup>33</sup> CAVV version 9 can be used with 3DS 1.0, This will allow the merchant name and amount to be embedded in the CAVV.

<sup>34</sup> Visa has defined a method for EMV 3DS 2.1.0 to support 3RI purchase transactions. Please note this approach is specific to Visa cards and is not included in the EMV 3DS specification.

<sup>35</sup> New functionality in EMV 3DS 2.2 that allows for authentication of cardholders independent from the purchase flow. More information, guidelines and details on testing due later in 2020.

Notable Features	3DS 1.0	3DS 2.1	3DS 2.2
Secure corporate payments (SCP) exemption	N	Y	Y
Acquiring Country Code (ACC) extension	N	Y	Y
Enhanced TRA plus data (100+ data elements)	N	Y	Y

Merchants should utilise the information received in the PReq/Pres exchange to determine the versions of EMV 3DS that are supported by the Issuer ACS.

EMV 3DS 2.2 introduces five new values for the 3DS Requestor Challenge Indicator field in the Authentication Request message to support application of exemptions and delegated authentication. For details of these indicators please refer to *the Visa Secure Program Guide*.

### 3.3.5 3DS Requestor Initiated (3RI)

The 3RI functionality allows the merchant to initiate an authentication request without the cardholder being present. This enables several merchant use cases. For example;

- It enables a merchant to obtain authentication data (CAVV, ECI) for transactions that have been previously authenticated and where the CAVV is no longer valid. For example, in the case of a delayed shipment which delays the authorization beyond 90 days. This allows the merchant to maintain their fraud liability protection under legitimate circumstances.
- It allows a merchant to obtain additional CAVVs associated with a single authentication interaction with the cardholder in the case of a split shipment where more than one authorization is needed.
- It allows an authorised entity in a Multi-Party Commerce scenario to request a CAVV on behalf of merchant(s).
- Non-payment (NPA) messages can be used to confirm an account is still valid for cardholder authentication.

Merchants and 3DS Server vendors should note the for some 3RI transactions the 3DS Server should provide 3DS Requestor Prior Transaction Authentication Information including:

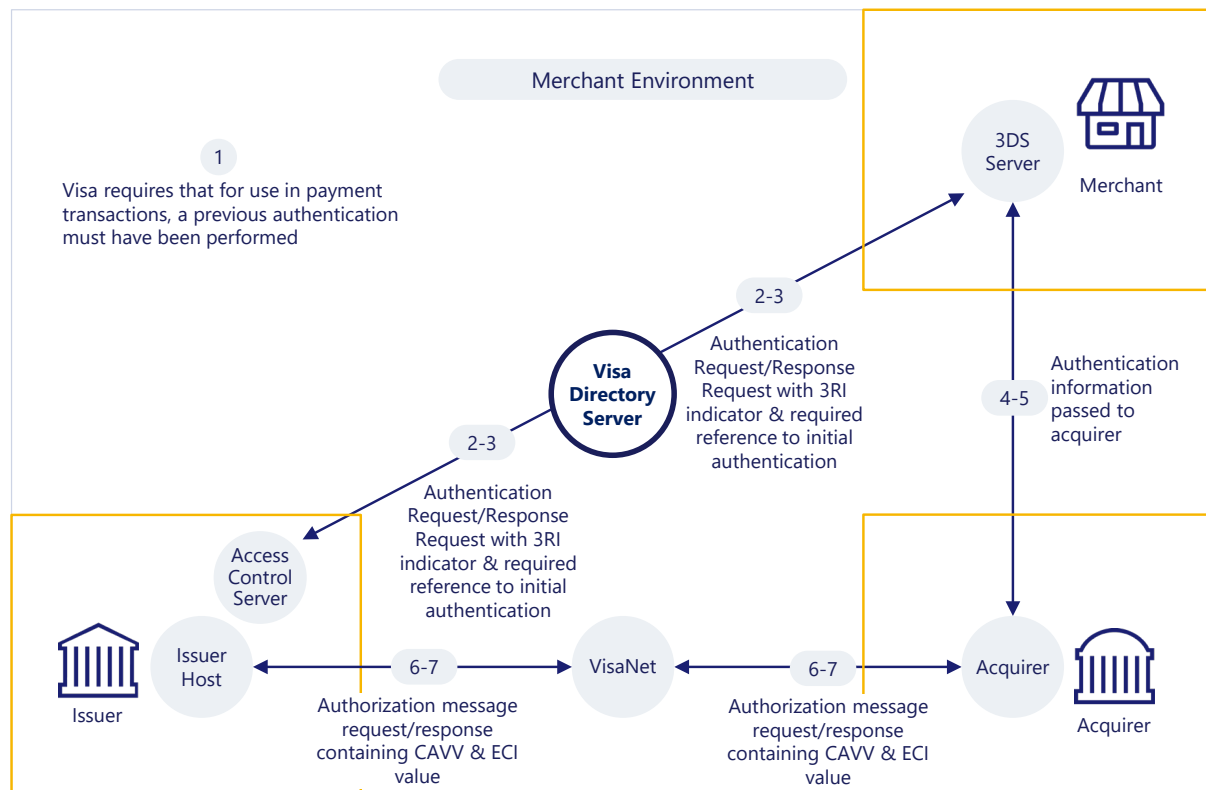
- 3DS Requestor Prior Transaction Authentication Method: This is the mechanism used by the Cardholder to previously authenticate to the 3DS Requestor
- 3DS Requestor Prior Transaction Authentication Timestamp: The date and time in UTC of the prior cardholder authentication
- 3DS Requestor Prior Transaction Reference: This data element contains an ACS Transaction ID for a prior authenticated transaction (for example, the first recurring transaction that was authenticated with the cardholder).

This additional data allows Issuers to identify the requests and improves risk management and provides a secondary evaluation of the previously authenticated transaction. The subsequent request to the Issuer may not always result in an approved transaction as the Issuer may reassess the transaction and merchants should cater for this in their systems.

Examples of where this may be used for specific transaction types are included in sections 5.3, 5.4 and 5.16.

Figure 8 below shows the standard 3RI flow.

**Figure 8: 3RI flow**



For more information on the application of 3RI please refer to sections 4.2.4.3 (Table 20 principle 3), 4.6.3 and 4.6.4.4.

### 3.3.6 EMV 3DS domains and components




Visa's EMV 3DS Program defines three distinct domains that interact to support authentication and authorization:

- The merchant/Acquirer Domain
- The Visa Interoperability Domain
- The Issuer Domain

These domains and the main components acting in each domain are illustrated in Figure 9 below:

**Figure 9: EMV 3DS domains and components**

Merchant / Acquirer Domain	Visa Interoperability Domain	Issuer Domain
<p><b>3DS Server / 3DS SDK</b></p> <p>3DS Server (software)    3DS SDK (software)</p>	<p><b>Visa Directory Server</b></p> <p>Visa Directory Server</p>	<p><b>Issuer Access Control Server (ACS)</b></p> <p>Issuer ACS server</p>
<p><b>Merchant's E-Commerce Software</b></p> 	<p><b>Visa Attempts Service</b></p> <p>Visa Attempts Server</p>	
<p><b>Acquirer / Acquirer Processor</b></p> <p>Payment processing system</p>	<p><b>VisaNet</b></p> <p>VisaNet</p>	<p><b>Issuer / Issuer Processor Host System</b></p> <p>Issuer Host</p>

For more details on the domains and components, please consult *Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure* and *Visa Secure Issuer Implementation Guide for EMV 3-D Secure 2.0*.

**Table 9: The role of the main components**

Component	Role
3DS Requestor	The initiator of the EMV 3-D Secure Authentication Request. For example, this may be a merchant.
3DS Client	The consumer-facing component allowing consumer interaction with the 3DS Requestor for initiation of the EMV 3-D Secure protocol.
3DS Server	The 3DS Server provides the functional interface between the 3DS Requestor Environment flows and the DS. The 3DS Server is responsible for: <ul style="list-style-type: none"> <li>Collecting necessary data elements for 3-D Secure messages</li> <li>Authenticating the DS</li> <li>Validating the DS, the 3DS SDK, and the 3DS Requestor</li> <li>Ensuring that message contents are protected</li> </ul>
3DS Requestor App	An App on a Consumer Device that can process a 3-D Secure transaction through the use of a 3DS SDK. The 3DS Requestor App is enabled through integration with the 3DS SDK
3DS Requestor Environment	The 3DS Requestor-controlled components (3DS Requestor App, 3DS SDK, and 3DS Server) are typically facilitated by the 3DS Integrator. Implementation of the 3DS Requestor Environment will vary as defined by the 3DS Integrator

Component	Role
3DS SDK	The mobile-device-side component of 3DS is the 3DS Mobile SDK. 3DS Requestors integrate this SDK with their mobile commerce or 3DS Requestor app and the SDK facilitates the sending and receiving of 3DS messages and the displaying of challenge screens to the cardholder
3DS Integrator	An EMV 3-D Secure participant that facilitates and integrates the 3DS Requestor Environment, and optionally facilitates integration between the Merchant and the Acquirer
Directory Server (DS)	The DS performs a number of functions that include: <ul style="list-style-type: none"> <li>• Authenticating the 3DS Server and the ACS</li> <li>• Routing messages between the 3DS Server and the ACS</li> <li>• Validating the 3DS Server, the 3DS SDK, and the 3DS Requestor</li> <li>• Defining specific program rules (e.g., logos, time-out values)</li> <li>• Onboarding 3DS Servers and ACSs</li> <li>• Maintaining ACS and DS Start and End Protocol Versions and 3DS Method URLs</li> <li>• Interacting with VTS to de-tokenize messages originating from tokens</li> </ul>
Issuer Access Control Server (ACS)	The ACS contains the authentication rules and is controlled by the Issuer. ACS functions include: <ul style="list-style-type: none"> <li>• Verifying whether a card number is eligible for 3DS authentication</li> <li>• Verifying whether a Consumer Device type is eligible for 3DS authentication</li> <li>• Authenticating the cardholder or confirming account information</li> </ul>
Visa Attempts Server	Stands in for the Issuer's ACS and responds to the 3DS Requestor if the Issuer's ACS is unavailable
VisaNet	Routes 3DS messages between the appropriate 3DS Requestor and Issuer ACS

For a more comprehensive definition of EMV 3DS terms please refer to the EMV 3-D Secure Protocol and Core Functions Specification Version 2.2 Table 1.3.

### 3.3.7 The EMV 3DS messages and process flow

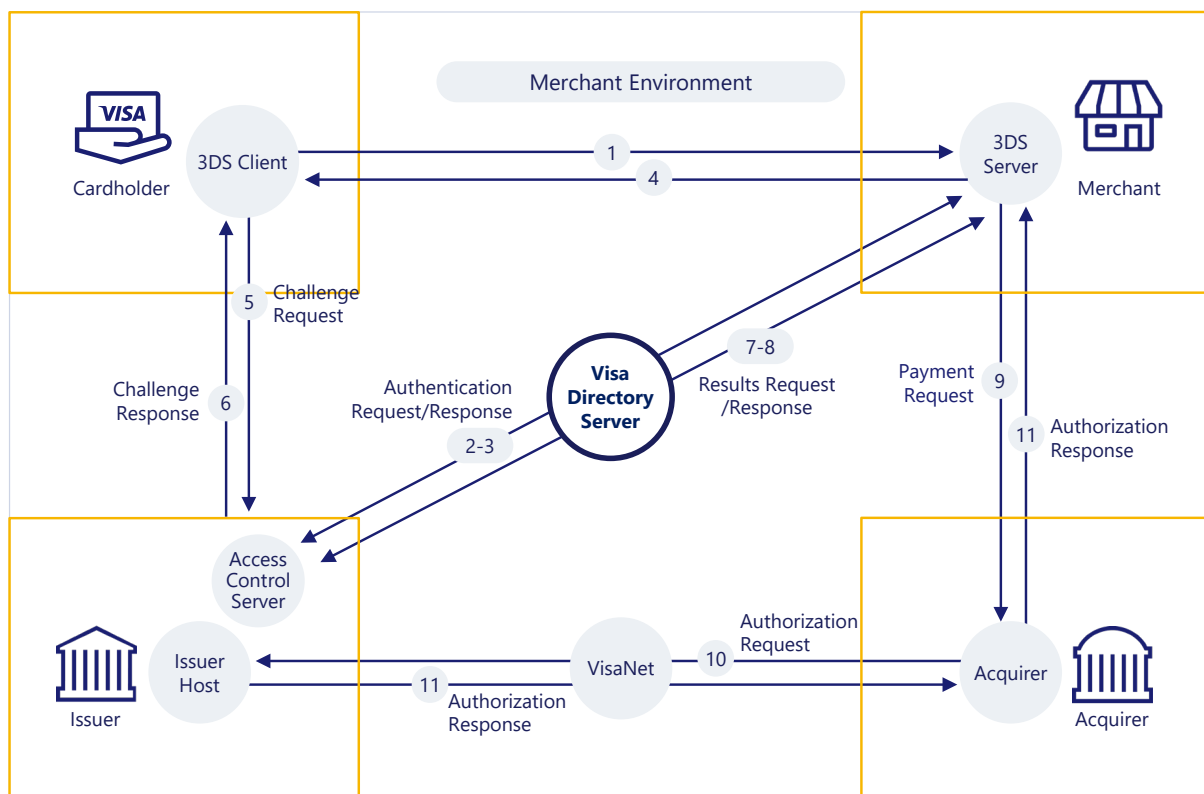


EMV 3DS enables merchants to send a message to an Issuer to carry out the authentication process.

The environment and basic message flow that comprises EMV 3DS and underpins both the frictionless and challenge flows is summarized in Figure 10. Familiarity with this will help readers understand the concepts around application of EMV 3DS, discussed in this guidance.



**Figure 10: The EMV 3DS secure environment and message flows**



EMV 3DS supports two primary authentication flows:

- Frictionless Flow: occurs when the Issuer authenticates the cardholder without cardholder involvement by evaluating the transaction’s risk level using Risk Based Authentication (RBA)
- Challenge Flow: occurs when the Issuer assesses the risk of the transaction during the frictionless flow and determines that the transaction requires additional cardholder authentication through application of a SCA challenge

How the 3DS authentication process works:

- Step 1: The cardholder initiates the transaction
- Step 2: The merchant’s 3DS Server initiates an authentication request by sending an Authentication request (AReq) message via the Visa Directory Server to the Issuer’s ACS. This message contains all the data elements that the Issuer requires to risk assess the transaction. It may also contain indicators requesting that an exemption is applied
- Step 3: The Issuer’s ACS undertakes a risk-based assessment of the transaction using the data elements provided and determines whether the transaction is out of scope/an exemption can be applied or an SCA challenge is required. The ACS responds via the DS to the 3DS Server with an Authentication Response (ARes) message advising that either the cardholder is authenticated, or further cardholder authentication is required

- Step 4: If further authentication is required, a SCA challenge is triggered and the cardholder provides additional information
- Step 5: A Challenge Request (CReq) message is sent between the 3DS SDK or 3DS server and the ACS with the additional authentication information provided by the cardholder
- Step 6: A Challenge Response (CRes) message is sent by the ACS in response to the CReq message indicating the result of the cardholder authentication
- Step 7: Results Request Message (RReq) is sent by the ACS via the DS to transmit the results of the authentication transaction to the 3DS Server
- Step 8: A Results Response Message (RRes) is sent by the 3DS Server to the ACS via the DS to acknowledge receipt of the Results Request message
- Step 9: If the cardholder is successfully authenticated, the merchant sends a payment request to the Acquirer, along with the ECI and CAVV
- Step 10: The Acquirer sends an authorization request to the Issuer which is provided along with the ECI and CAVV
- Step 11: The Issuer responds via the Acquirer with the authorization response (approve or decline)

Steps 5 to 8 are only required if a SCA challenge is required.

Note, while the Issuer's ACS will respond to Authentication requests on behalf of the Issuer, the Issuer will set the rules and policies applied by the ACS and the ACS may refer some transactions to the Issuer for review. The Issuer may also manage the application of an SCA challenge such as an SMS OTP or push message to a mobile banking app, where this is required.

For more detail on the messages, refer to the Visa Merchant/Acquirer and Issuer Implementation Guides for Visa's EMV 3DS Program.

### 3.3.8 Visa Authentication Data



Visa Authentication Data is used to communicate information about authentication between the Issuer ACS, the merchant, VisaNet, and the Issuer Host. Table 10 provides full details:

**Table 10: Visa authentication elements**

Data Elements	Created by	Purpose
Electronic Commerce Indicator (ECI)	Issuer ACS, or Visa's Attempts Server	Indicates the level of authentication that was performed on the transaction. The ECI value is passed to merchant and included by the merchant in the authorization request.
Cardholder Authentication Verification Value (CAVV)	Issuer ACS, or Visa's Attempts Server	Unique cryptogram generated for each 3DS authenticated transaction and linked to the transaction amount and payee. The CAVV is passed to the merchant and submitted with the authorization request to prove authentication has occurred.
CAVV Results Code (Field 44.13)	Issuer or VisaNet	Communicates the results of the CAVV verification performed during authorization (e.g. PASS/FAIL) and indicates if the CAVV was created by the Issuer's ACS, the Issuer's Attempts Server, or Visa's Attempts Service.
3-D Secure Indicator (Field 126.20)	VisaNet	Optional field that the Issuer or Acquirer can choose to receive in authorization. Communicates the 3DS version number and the EMV 3DS authentication method used to authenticate the cardholder. This can be used to improve risk assessment in authorization processing, reporting and analytics etc.

For more details on these data fields please refer to the *Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure*.

### 3.3.9 Risk Based Authentication



#### 3.3.9.1 Introduction to RBA

Risk Based Authentication (RBA) is a process that may be used by Issuers to risk assess and score 3DS transactions to reduce the volumes that require SCA. It enables Issuers to:

- Apply the TRA exemption to remote transactions (where their fraud rate is below the relevant PSD2 reference fraud rate threshold and they meet the other requirements of the TRA exemption)
- Risk assess Authentication Requests submitted via EMV 3DS with an Acquirer exemption indicator (EMV 3DS specification version 2.2 onwards) and decide whether to apply the right of final say over whether SCA should be applied to a transaction
- Reduce false declines

Visa considers RBA to be critical to reducing unnecessary challenges and friction and has issued a global rule mandating that Issuers support it.

RBA uses transaction data to assess fraud risk without the need for the cardholder to complete a SCA challenge. RBA is an integral element of EMV 3DS and enables “frictionless” authentication of low risk transactions. The EMV 3DS specification defines up to 135 data elements that can be included in the initial authentication request (AReq) message and used by the Issuer’s ACS fraud engine to assess each transaction with a high degree of confidence. For the latest version of data elements and their requirement please refer to the latest version of the *Visa Secure Program Guide*. The elements are fully defined in the EMVCo specification: EMV 3-D Secure Protocol and Core Functions Specification.

Where transaction risk is assessed as low, and the Issuer’s fraud rate is within the reference fraud rate for the transaction value, the Issuer may apply the TRA exemption to a remote transaction without the need to apply a challenge. Where the risk is not assessed as low, the Issuer’s fraud rate is outside the reference fraud rate, or the other requirements of the TRA exemption are not met, a challenge will need to be completed.

### 3.3.9.2 Benefits of RBA

Risk Based Authentication has already delivered significant benefits in the markets where it has been deployed. In the UK in the pre-PSD2 environment, 95% of transactions that undergo a risk-based assessment have not required additional customer authentication. Since the introduction of a risk-based approach there has been a 70% reduction in abandonment rates. At the same time, fraud rates have fallen, indicating that risk-based assessments are an effective tool to detect and prevent fraud. The use of a significantly greater number of risk scoring data points under EMV 3DS will increase the effectiveness of RBA even further. Visa analysis shows that the addition of just one of those data points – device ID information – improves fraud detection rates by over two hundred percent. In cases where it is necessary to apply SCA, further strengthens the effectiveness of authentication. This is what Visa refers to as a “layered approach”.

### 3.3.10 Data elements



EMV 3DS also requires that merchants submit additional transaction data with the authentication request message. This data is used by Issuer’s ACS providers to analyse the risk of the transaction and can reduce the number of transactions for which SCA is applied. It is critical that this data is correctly formatted, consistent and of high quality in order to avoid Issuers having to apply SCA just because they have insufficient data to risk assess a transaction.

The Data Element Types supported with EMV 3DS include those listed in Table 11 below:

**Table 11: Example data types**

Category	Example
Transaction & Checkout Page Information	<ul style="list-style-type: none"> <li>• Cardholder Information (e.g. account number, billing/ shipping address)</li> <li>• Merchant Information (e.g., name, URL, ID, merchant country, MCC)</li> <li>• Transaction Info (e.g., dollar amount, transaction type, recurring/installment)</li> <li>• Device Information (e.g., browsers width, height, country, device channel: app-based browser)</li> </ul>
Authentication Information	<ul style="list-style-type: none"> <li>• 3DS Requestor Authentication method, date, time (i.e. cardholder "logged in" as guest or cardholder logged into merchant account)</li> </ul>
Prior Authentication Information	<ul style="list-style-type: none"> <li>• Prior Authentication method, time and date</li> </ul>
Merchant Risk Indicator	<ul style="list-style-type: none"> <li>• Pre-order indicator</li> <li>• Gift card amount, currency, count</li> <li>• Shipping &amp; delivery information</li> </ul>
Cardholder Account Information	<ul style="list-style-type: none"> <li>• Cardholder account age, date, change</li> <li>• Password change</li> </ul>
Device Information	<ul style="list-style-type: none"> <li>• Platform Type</li> <li>• Device Model</li> <li>• Browser/SDK</li> </ul>

Merchants should pay particular attention to the Browser IP, Shipping Address Postal code, Billing Address Postal code, and Address match indicator as key fields. However, in general, the more quality data that the merchant is able to supply over time (regardless if it is optional or required), the more it can assist in the risk analysis of the transaction.

A further critical factor in the gathering of data is the use of the 3DS Method URL. If a 3DS Method URL is specified, then merchants must use this for the appropriate flows.

### Requirement

Merchants are required to submit the required data elements in the EMV 3DS authentication request message. Provision of this data allows issuers to make optimum risk decisions and minimises unnecessary applications of SCA.

Visa has introduced a rule to ensure that minimum data provision standards are applied. For the latest version of data elements and their requirement refer to the latest version of the *Visa Secure Program Guide*.

### 3.3.11 Token transactions and 3DS



3DS authentication is supported for card on file, e-commerce, and application-initiated e-commerce transactions using network tokens. This uses two separate cryptograms in the authorization message, the TAVV token cryptogram for token validation, and the 3DS CAVV cryptogram for cardholder authentication. Visa requires that Acquirers submit both the TAVV token cryptogram and 3DS CAVV cardholder authentication cryptogram in authorization requests for token-based transactions with 3DS.

Acquirers that participate in Visa Token Service (VTS) and 3DS are required to support the TAVV cryptogram data in Field 126.8—Transaction ID (XID) in combination with the 3DS CAVV cryptogram data in Field 126.9—Usage 3: 3-D Secure CAVV, Revised Format for token-based transactions with 3DS.

### 3.3.12 UX considerations

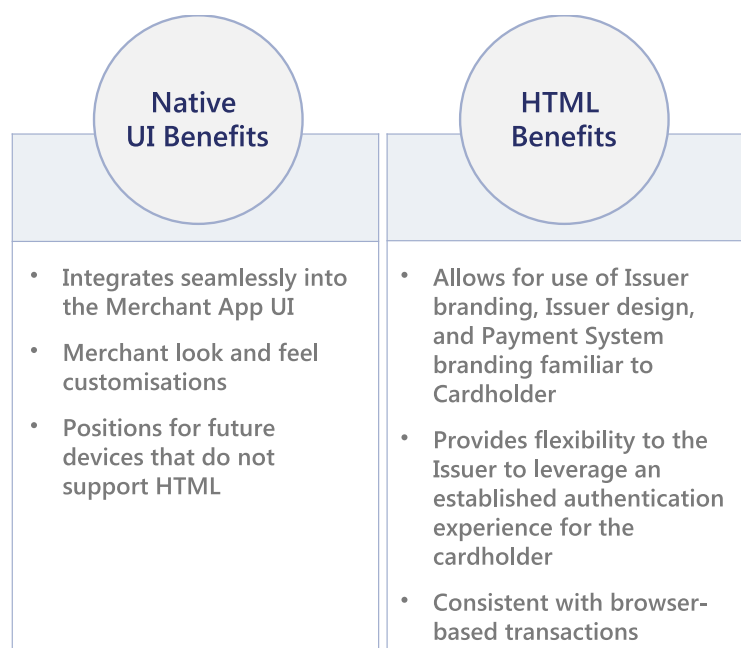


EMV 3DS provides significantly enhanced user experiences through:

- Enhanced support of mobile devices and native app environments
- Use of RBA to reduce unnecessary challenges
- Lower friction challenge methods including biometrics
- Challenge flows that are better integrated into the checkout flow with options for merchant branding of some elements

Consumer research carried out by EMVCo has shown that the presence of network and bank logos conveys more clearly to the cardholder the trusted party performing authentication. Furthermore, the standard offers the flexibility to offer two options for in-app: 1) native UI 2) HTML, more details are given in Figure 11.

**Figure 11: Relative benefits of native UI v HTML**



It should be noted that while the merchant has the option to brand aspects of the native UI and customize the wording of the header, the content of the challenge messages is determined by the Issuer and served by the Issuer’s ACS. For more information please refer to Section 4.6.1 and to the 3DS UX Guidelines available on the Visa Developer Center<sup>36</sup>.

### 3.3.13 EMV 3DS on different platforms



EMV 3DS supports desktop browser and mobile platforms with both HTML and native app interfaces as well as games consoles, allowing seamless support of in-game purchases.

### 3.3.14 The co-existence of 3DS 1.0 and EMV 3DS



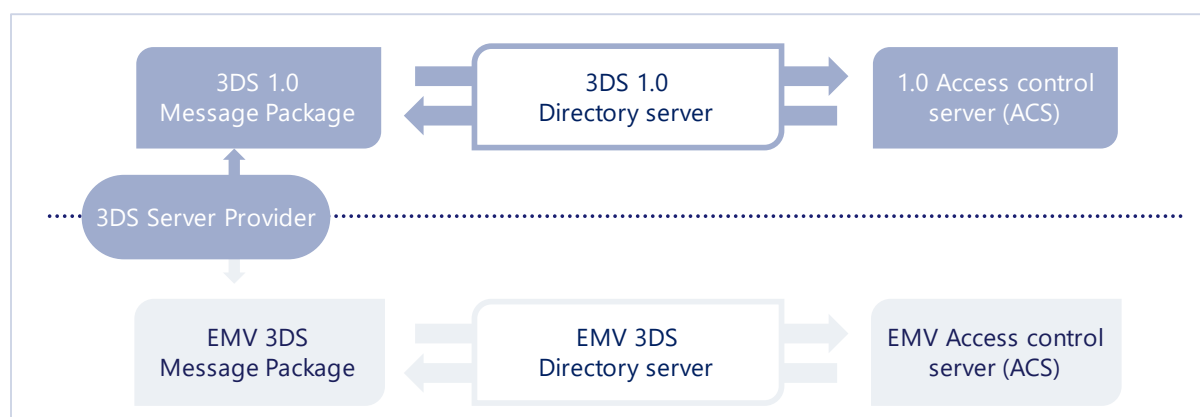
EMV 3DS and 3DS 1.0 are two separate, distinct protocols, supported by two separate Directory Servers that will co-exist independently in parallel for a transition period. Both protocols will continue to be supported until EMV 3DS reaches maturity in the market. Visa expects to announce a sunset date for 3DS 1.0, after which 3DS 1.0 will no longer be supported, in due course.

Merchants should always aim to use the highest version of 3DS supported by the Issuer.

During the transition period, when not all Issuers support EMV 3DS, merchants supporting EMV 3DS will be able to determine which version of 3DS an Issuer supports. The merchant’s 3DS Server Provider can request an update, called a Preparation Request (PReq) message, from the Visa Directory Server for the latest list of BINs and account ranges that are supported by the different 3DS protocol versions. 3DS Server Providers should utilize this protocol version information to package messages accordingly and send to appropriate 3DS Directory Server as illustrated below.

In order to obtain optimal authorization performance, merchants should be using the daily Preparation Request (PReq) / Preparation Response (PRes) message in EMV 3DS to ascertain which version of 3DS each Issuer is enabled on.

**Figure 12: Routing of authentication request messages during the transition period**



<sup>36</sup> <https://developer.visa.com/pages/visa-3d-secure#introduction>

As stated in section 3.3.2.2, the Visa European activation date for EMV 3DS 2.1 was 14 March 2020. From this date, merchants receive fraud liability protection for both successful and attempted 3DS transactions with EMV 3DS 2.1. Fraud liability protection for merchants using 3DS 1.0 will end on 17 October 2021. After this date, merchants must use EMV 3DS in order to benefit from fraud liability protection.

For more information on the Visa Attempts Server see Section 4.7.1.

The potential combinations of responses and liabilities are summarized in Table 12 below.

**Table 12: 3DS transaction liability status after 14 March 2020**

Merchant 3DS Version	Issuer 3DS version	Issuer availability or Visa 3DS Attempts Stand In <sup>37</sup>	Fraud liability under Visa Rules
3DS 1.0	3DS not supported	Visa Attempts Server	Issuer (ECI 06) <sup>38</sup>
3DS 1.0	3DS 1.0	Issuer available	Issuer (ECI 05) <sup>38</sup>
3DS 1.0	3DS 1.0	Issuer unavailable – Visa Attempts Server	Issuer (ECI 06) <sup>38</sup>
EMV 3DS 2.1	EMV 3DS not supported (Issuer not supporting 3DS at all or supporting 3DS 1.0 only)	Visa Attempts Server	Issuer (ECI 06)
EMV 3DS 2.1	EMV 3DS 2.1	Issuer available	Issuer (ECI 05)
EMV 3DS 2.1	EMV 3DS 2.1	Issuer unavailable – Visa Attempts Server	Issuer (ECI 06)

### Best Practice

Merchants are strongly advised to send authentication requests to the highest version of 3DS supported by the Issuer, including during the transition period to EMV 3DS when not all Issuers support EMV 3DS. This enables issuers to properly risk assess each transaction. 3DS Server providers receive up to date protocol information to enable transactions to be routed to the correct DS.

<sup>37</sup> Some card ranges and message types are excluded from attempts processing. See the Visa Secure Program Guide for further information.

<sup>38</sup> Only applies until 17 October 2021.



Issuers should note that under the terms of EMV 3DS activation in Europe, merchants can choose to authenticate with EMV 3DS, regardless of the state of Issuer readiness. When this happens and the Issuer is not yet enabled, those transactions will proceed to authorization as a ECI 06. Issuers need to introduce proportionate risk control measures in their authorization fraud detection systems to manage fraud levels for these transactions. A blanket decline strategy of ECI 06s by Issuers is not permitted under the Visa rules. Managing the risk of ECI 06s using a statistical based fraud detection system, in conjunction with fraud rules, allows for a more accurate and proportionate response, with fewer false positives.

Issuers are advised to review their management of electronic commerce indicator (ECI) 6 Authorization responses should the Issuer's ACS be unavailable to respond to an authentication request once regulatory enforcement is in effect.

Issuers may want to consider:

- Their business continuity plans when managing authorization responses following the merchant's attempt to enable SCA compliance, in order to minimize the impact to consumers and reduce customer complaints.
- The application of exemptions, where appropriate to the transaction, such as TRA or Low Value.

### 3.3.15 3DS Testing



Ecosystem participants are reminded to ensure adequate testing and validation occurs prior to going live with EMV 3DS.

Issuers and merchants must ensure that their ACS and 3DS Service vendors respectively have completed the full Visa product certification testing (vendor certification) for the version of EMV 3DS protocol they wish to process on and can support additional PSD2 use-cases to enable compliant implementations for: optimized payment flows, customer experience and approval rates.

This includes use-cases where participants make use of exemptions to SCA and send transactions straight to the authorization flow, using either the MIT framework, or Field 34, to indicate the exemption being applied. Issuers and Acquirers are reminded to ensure they have fully tested the use of the fields used in these instances.

Issuers are reminded that Visa cannot accept project requests unless your ACS vendor has completed their full vendor testing and certification for all mandatory test cases.

Issuers and merchants should work with their ACS and 3DS vendors respectively to establish testing capabilities and a test plan to validate their processing for each version of the protocol you are enabling, this should include:

- Validation of EMV 3DS authentication message processing in all authentication flows including frictionless, challenge, exemptions, and errors
- Validation of the user experience and screen rendering
- Validation of latency and abandonment

To further assist ecosystem participants' enablement prior to go-live, Visa is making available testing facilities for participants. For more information about these facilities please contact your Visa Representative.

## 3.4 Visa's PSD2 solutions using Visa Token Service (VTS)



Clients can use the Visa Token Service (VTS) and its capabilities to help meet their PSD2 SCA obligations. This section briefly describes the solution and the features it offers.

### 3.4.1 The Visa Token Service (VTS)

VTS is a technology from Visa which replaces sensitive account information, such as the 16-digit primary account number, with a unique digital identifier called a token. The token may be issued with domain controls which limit its use to the merchant, channel or consumer device to which it was issued.

Visa Tokenization helps reduce fraud and improve card authorization rates. VTS offers a robust platform with additional value-add services & features to enhance the payment flow throughout the ecosystem. It provides a complete integrated set of tokenization tools and capabilities for merchants, Token Requestors<sup>39</sup>, Issuers, Acquirers and processors.

VTS can help address the requirements of PSD2 through:

- Maximizing the ability of PSPs to apply the TRA exemption
- Facilitating the application of SCA between customers and qualifying delegates participating in the Visa Delegated Authentication Program (see Section 3.8 below)
- Supporting dynamic linking through the token cryptogram

### 3.4.2 The Visa Cloud Token Framework

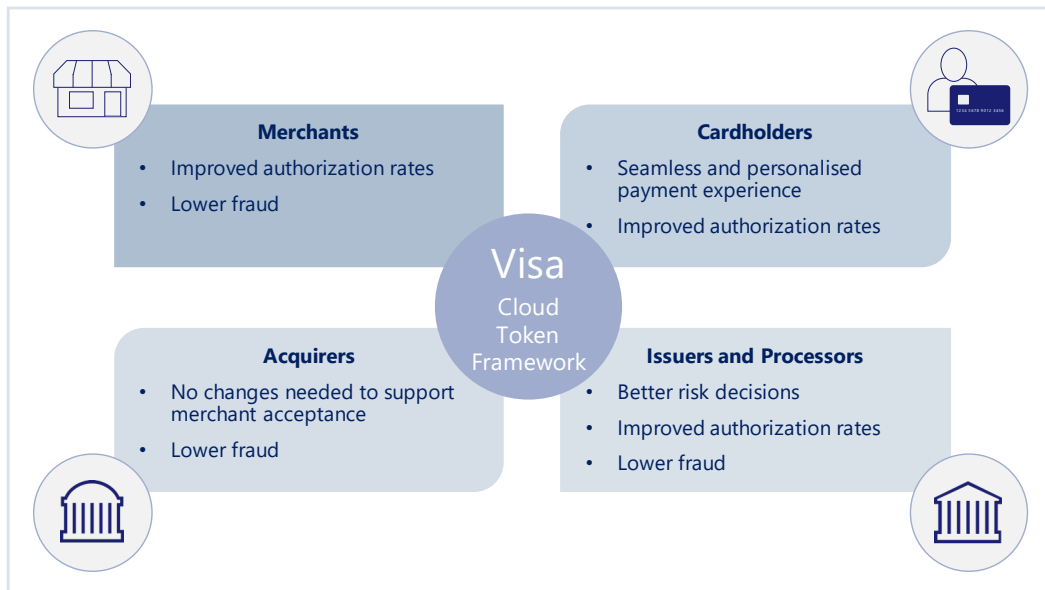
The Cloud Token Framework is a global framework which brings the advantages of device-based tokens and applies them to e-commerce and card-on-file tokens. With the features of device binding and cardholder verification, CTF results in a better quality credential as well as providing greater certainty and confidence for the payment ecosystem.

As with 3DS, the Cloud Token Framework delivers important benefits to all stakeholders. These are summarized in Figure 13 below:

---

<sup>39</sup> Token Requestors are entities that request payment tokens for end-users, for example digital wallet providers, payment enablers or merchants.

**Figure 13: Cloud Token Framework benefits**



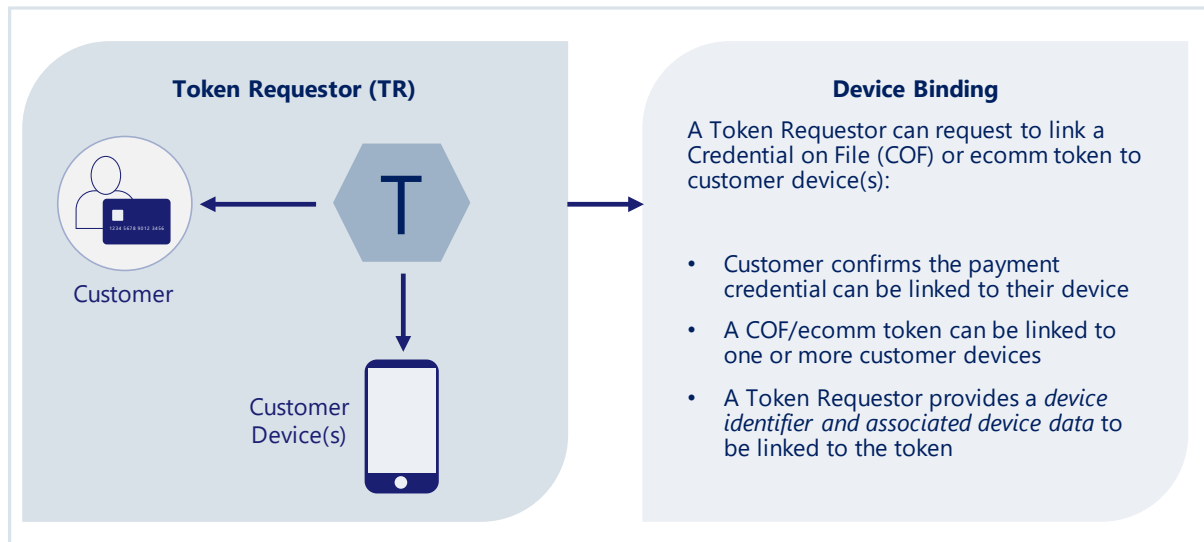
**3.4.2.1 Features of the Cloud Token Framework**

Device Binding and Cardholder verification are two key features of the Cloud Token Framework. The below sections describe these features, as well as other functions and benefits, in further detail:

**3.4.2.1.1 Device Binding**

Device binding enables e-commerce and/or card-on-file tokens which are provisioned to the consumer’s account to be bound to multiple trusted devices.

**Figure 14: Principles of Device Binding**



The Device Binding process verifies that the Issuer’s cardholder has possession of the device on which the token is being used or provisioned. It is done through performing Issuer authentication and may occur during token provisioning or as a standalone action initiated by a Token Requestor after token provisioning has occurred. The Token Requestor sends the request to VTS to bind the device, passing the data that it has gathered from the device and requesting that the device is bound to the token credential that has been previously issued. If

the bound token is subsequently to be used as a possession factor for SCA, the Issuer must perform SCA in order to verify the customer before the binding of the device to the token is finalized.

### 3.4.2.1.2 Token Requestor-initiated cardholder verification

This allows the Token Requestor to request cardholder verification to be applied for any already provisioned e-commerce or credential on file token. Token Requestors may request cardholder verification at any time, whether or not a device binding request has been performed, to explicitly establish that the Token Requestor’s customer is the Issuer’s cardholder. If the verification is used to enable subsequent delegated authentication to the token requestor, then the cardholder verification performed should meet SCA requirements.

### 3.4.2.1.3 The Role of tokenization in the Visa Delegated Authentication Program

The CTF can be used when an Issuer elects to delegate authentication to a third party. Initial e-commerce use cases for delegated authentication facilitated by token transactions include:

- In-app transactions,
- E-commerce transactions from Token Requestors
- E-commerce transactions using 3DS

Specifically CTF:

Enables third party delegates to provide information to Issuers on the authentication method applied at the time of the transaction. The factors used are sent in the payment transactions via field F123, Dataset id 68 tags 83 and 84.

- Caters for dynamic linking requirements through the use of a token-based cryptogram (TAVV). The TAVV supports linking of the transaction to the merchant (payee) and the transaction amount using an encrypted, verifiable authentication code
- Provides Issuers with the ability to configure specific qualifying merchants and Token Requestors they agree to accept as delegates under the Visa Delegated Authentication Program

Table 13 below summarises key fields for Visa Delegated Authentication for token transactions and dynamic linking and provides token-specific notes

**Table 13: System Fields for Visa Delegated Authentication**

Field	Tag Position/Field Value	Sent from Acquirer?	Sent to Issuer?	Token-Specific Information
<b>F34</b>	Dataset 4A, Tag 8A— Delegated Authentication	Yes	Yes (conditionally)	<ul style="list-style-type: none"> <li>• For token transactions, Acquirers do not have to set this field. Visa Token Service (VTS) will extract the delegated authentication indicator from the transaction cryptogram (Token Authentication Verification Value [TAVV]) and set this value in F34 when sending to the Issuer.</li> <li>• VTS will ignore the Acquirer-populated value for this field; instead, this value is set by VTS based on the TAVV.</li> </ul>

Field	Tag Position/Field Value	Sent from Acquirer?	Sent to Issuer?	Token-Specific Information
				Note: For device-based proximity payment token transactions, the DA indicator will not be set in Field 34.
<b>F126.5</b>	<p>Visa Merchant Identifier (VMID)</p> <p>(It is optional for Issuers to receive this field.)</p>	Yes	Yes	<ul style="list-style-type: none"> <li>For 3-D Secure (3DS) token transactions, this field identifies the delegate.<sup>40</sup></li> <li>For non-3DS token transactions, the token requestor will act as the delegate and is identified by the Token Requestor ID (TRID). The VMID is not relevant in this case.</li> </ul> <p>Note: For non-3DS token transactions, Acquirers do not have to set this field. If this field is provided by the Acquirer, Visa will send it to the Issuer (i.e., Visa will not drop this field).</p>
<b>F126.8</b>	If CAVV and TAVV are present, then TAVV data is in this field. If only the TAVV is present, then the Acquirer can populate this field or Field 126.9.	Yes	Optional if TAVV	<ul style="list-style-type: none"> <li>For non-3DS token transactions, the TAVV will contain delegation intent set by the token requestor. Visa will dynamically set the delegated authentication indicator in F34 based on the TAVV.</li> </ul>
<b>F123</b>	<p>Dataset ID 68:</p> <ul style="list-style-type: none"> <li>Tag 81—Token User Identifier</li> <li>Tag 83—Token Authentication Factor A</li> <li>Tag 84—Token Authentication Factor B</li> <li>Tag 85—Token Authentication Amount</li> </ul>	No	Yes	<ul style="list-style-type: none"> <li>These values will be set in F123 based on the incoming TAVV.</li> <li>Token Authentication Factors A and B are set by the delegate to inform the Issuer how SCA was performed.</li> <li>Token User Identifier (payee identifier) and Token Authentication Amount are provided for PSD2 dynamic linking purposes.</li> <li>Refer to Article 3.3—<i>Changes to the Visa Token Service to Support Cloud Token Framework</i> in the October 2019 Global Technical Letter for further details.</li> </ul>

Note: Token transactions will require a TAVV unless they are merchant-initiated transactions (MITs). MITs are out of scope for SCA; therefore, delegated authentication does not apply. The above table does not include situations where the TAVV is not present.

For more information on use of the CTF to support delegated authentication, please refer to Visa Business News: Authentication of Token Transactions with Visa Delegated Authentication 29 August 2019.

<sup>40</sup> For token transactions with 3DS, delegated authentication transactions will be processed based on processing rules in Article 9.1.2 of the October 2019 Global Technical Letter.

For more information on the Visa Delegated Authentication Program see section 3.8 below, the *Visa Delegated Authentication Program Implementation Guide* and *Article 9.1.2 in Oct 2019 GTLIG*.

#### 3.4.2.1.4 The role of The Cloud Token Framework in Optimising application of the TRA exemption

As the CTF provides a lower risk credential than using a PAN, it may facilitate lower overall fraud rates, providing stakeholders with an opportunity to maximise their use of the TRA exemption. Furthermore each individual transaction facilitated with a cloud token has a greater likelihood of being assessed as lower risk and is therefore more likely to qualify for the TRA exemption.

### 3.5 Visa Rules & policies for authentication & authorization under PSD2



#### 3.5.1 Visa Rules relevant to authentication and authorization PSD2

A number of existing and new Visa Rules govern the application of SCA under PSD2. These rules define some specific requirements that Issuers, Acquirers and merchants must comply with when applying or requesting authentication and authorization. The rules aim to ensure:

- That transactions are correctly identified in the authentication and authorization process flows according to whether and how SCA should be applied
- That transactions are not incorrectly authorized or unnecessarily declined due to:
  - Issuers, Acquirers or merchants responding incorrectly to relevant indicators
  - Legitimate exemptions not being recognized
- That transactions that are out of scope of the SCA regulation or otherwise do not require an Issuer to apply SCA are recognized
- That Issuers are encouraged to balance risk management with the minimization of friction

These rules which include support of exemption and out of scope indicators in authorization messages and minimum standards for authentication abandonment, the need for Issuers to apply challenges when requested by a merchant, risk analysis technology, the application of biometrics and minimum data requirements, will all contribute to a smoother authentication experience and lower fraud rates.

Relevant rules are included in *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements*.

#### 3.5.2 Visa EMV 3DS Performance Program

All parties in the ecosystem are required to adhere to the strict requirements detailed in the Visa document *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements* and Visa has implemented a performance program to actively monitor key performance metrics and ensure transaction approval rates are maintained at the highest level. Further information on metrics that Visa will track under the program and the commencement dates for the performance program are detailed in the document referred to above. Issuers and Acquirers are reminded

to familiarize themselves with that document and other Visa SCA publications to ensure they are compliant and providing the best level of service to consumers.

Visa will update these requirements from time to time and reserves the right to determine the application of any given requirement, as applicable.

## 3.6 Visa Trusted Listing



### 3.6.1 Introduction to Visa Trusted Listing

Visa has developed the capability for customers to speed checkout at preferred digital merchants by adding merchants to their Trusted List.

When making a purchase with a participating merchant, a customer will be asked during checkout if they would like to add this merchant to their Trusted List. Once SCA has been completed, the merchant will, subject to the Issuer's approval, be added to the customer's Trusted List.

The customer can also add a merchant to their Trusted List outside of the transaction flow, for example in a merchant's wallet page when saving a card on file, or after the transaction completes.

Subsequent transactions with merchants that have been added to a customer's Trusted List should generally not require SCA.

The customer can manage their Trusted List with their Issuer via the Issuer's customer call centre or the Issuer's web or mobile banking application.

### 3.6.2 How Visa Trusted Listing works

#### 3.6.2.1 Adding a merchant to the Trusted List

Customers may add a participating merchant to their Trusted List:

- While the customer is shopping online with the participating merchant
- Outside the purchase flow

When a customer is signed in and shopping at an online merchant, the merchant can display messaging informing the customer about the option to add the merchant to the Trusted List. During a purchase, the merchant will send a request through EMV 3DS 2.2 for the Issuer to give the customer the option to add the merchant to their Trusted List. The Issuer's ACS provider will display the Trusted Listing option to the customer. If the customer agrees, the customer will then authenticate for both adding the merchant to the Trusted List and for the purchase. Once authentication is successful, the merchant will be added to the customer's Trusted List.

Visa Trusted Listing also allows the merchant to enable the customer to add a merchant to the Trusted List outside of the transaction flow. For example, the merchant can display messaging about adding the merchant to their Trusted List on their wallet page, when saving a card on file, or after the transaction completes. The merchant will send a request through EMV 3DS 2.2 for the Issuer to give the customer the option to add that merchant to their Trusted List. If the customer agrees to add the merchant to their Trusted List, the customer must authenticate for

the addition. Once successful, the merchant will be added to the customer's Trusted List. Future purchases at that merchant will typically not require SCA.

A customer can also add a participating merchant to their trusted list through their Issuer (see section 3.6.2.2 below).

### 3.6.2.2 Managing the Trusted List

With Visa Trusted Listing, customers will create and maintain their trusted list with their Issuer. In addition to adding merchants via the EMV 3DS 2.2 flows described above, they can view their Trusted List and add and remove merchants to and from their Trusted List via their browser-based on-line banking service or mobile banking app, or via the Issuer's call centre.

A full description of these flows, including the mandatory fields and values can be found in the *Visa Trusted Listing Program Implementation Guide*

### 3.6.3 Benefits

The Visa Trusted Listing Program provides an effective framework for enabling the PSD2 trusted beneficiaries exemption. This can deliver important benefits to both merchants and Issuers.

Merchants with a low fraud rate may benefit from:

- The ability to provide a seamless purchasing experience for their regular customers without the need for an SCA challenge, regardless of transaction value
- The ability to use the trusted beneficiaries exemption for payment use cases where it may be difficult to apply SCA
- Achieving higher sales conversions post-PSD2 with minimal incremental investment
- Implementing a program that largely utilizes existing technology and so can be adopted with minimal technology development and implementation overhead

Issuers may benefit from:

- Providing their customers with a simple and secure way of ensuring that they don't get challenged when they shop at trusted merchants
- Putting their customers clearly in control of their Trusted Lists by providing a seamless way of adding and removing merchants from Trusted Lists and checking a merchant's status
- Having the confidence that merchants enrolled in the Program have, and will have strong incentives to maintain, a low fraud rate
- Achieving higher sales conversions post-PSD2 with minimal incremental investment
- Implementing a Program that largely utilizes existing technology and so can be adopted with minimal technology development and implementation overhead
- Having the ability to still apply SCA if they are concerned about the risk profile of a particular transaction



### 3.6.4 Components of the Program

There are four key components to the Visa Trusted Listing Program:

- **Rules Framework:** The Visa Rules and the *Visa Trusted Listing Program Implementation Guide* provides the framework for Issuers and Acquirers to participate in the Visa Trusted Listing Program
- **Program Enrollment:** Acquirers that choose to participate will identify and register eligible merchants that meet the qualification criteria
- **Transaction Identification:** A merchant must submit the required data fields to indicate that a transaction was submitted for the Visa Trusted Listing Program
- **Program Compliance:** Participants must comply with a fraud rate for transactions that have participated within Visa Trusted Listing

### 3.6.5 Technical Dependencies

In order to support Visa Trusted Listing, stakeholders must be able to support certain technical standards and message fields for authentication and authorization, notably:

- Merchants and their 3DS Servers will need to be enabled for EMV 3DS 2.2 Merchants will need to work with their 3DS Server provider to ensure logic is in place to know when to flag a transaction for Visa Trusted Listing
- Issuers and their ACS providers will need to be EMV 3DS 2.2 ready to accept Visa Trusted Listing requests
- Stakeholders will need to support certain V.I.P. system fields and values in authorization

For more information on the application of the trusted beneficiaries exemption please see Section 4.5.3. For detailed implementation guidance, including the Program qualification criteria and participant enrollment processes, please refer to the *Visa Trusted Listing Program Implementation Guide*.

## 3.7 Visa Delegated Authentication



### 3.7.1 Introduction to Visa Delegated Authentication

PSD2 allows PSPs to outsource authentication to an entity to conduct SCA on their behalf. Visa's Delegated Authentication program 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. PSPs should be aware that they remain fully liable for their own regulatory compliance.

### 3.7.2 Benefits

Visa Delegated Authentication is designed to support the needs of all stakeholders in the ecosystem.

Delegates such as merchants who have invested in their fraud infrastructure and are best-in-class at managing fraud, including having the capability to apply SCA, are able to deliver a

consistent consumer payment experience when SCA is required, whilst maintaining relevant security controls.

Issuers may benefit from higher sales conversions post-PSD2 with minimal incremental investment. Visa manages the Program and provides the Issuer and Acquirer with oversight and supervision so that SCA can be performed and Issuers are capable of meeting their regulatory requirements and so that fraud is strictly and consistently managed.

The Program largely relies on existing technology and so has few additional technical requirements.

### 3.7.3 Components of the Program

There are four key components to Visa Delegated Authentication:

- 1. Rules and Liability Framework:** The *Visa Rules* and the *Visa Delegated Authentication Implementation Guide* provide the framework for Issuers to delegate SCA to participating Acquirers and in turn their qualified Delegates. Participating Acquirers will identify Delegates that meet the qualification criteria and, if approved by Visa, those Delegates may then conduct SCA on the Issuers' and Acquirers' behalf. Token Requestors may also become delegates in their own right. Issuers should familiarize themselves with the Program, its alignment to their internal policies, and identify any steps they should take before the Program commences. Issuers are automatically enrolled in the program but various opt out options are available.
- 2. Program Qualification:** Acquirers that choose to participate will identify and qualify potential Delegates that meet the qualification criteria and work with them to evidence how their authentication capabilities are compliant and to obtain their agreement to the requirements of the Program through the Readiness Questionnaire. Token requestors may submit their Readiness Questionnaire directly to Visa.
- 3. Transaction Identification:** On a per transaction basis, the delegated entity will flag to the Issuer that SCA was performed through EMV 3DS (2.2 only) or VTS.
- 4. Program Compliance:** Issuers and Acquirers are required to maintain fraud and risk monitoring and Issuers may request additional SCA or decline if a serious risk is identified. Delegates are required to meet fraud performance requirements upon entry and on an ongoing basis and are required to apply SCA in line with all applicable regulatory requirements.

The Visa Delegated Authentication Program provides delegates with the opportunity to use either 3DS or VTS for the establishment of the authentication code needed for dynamic linking, together with indicators as to the identity factors used as part of the delegated authentication.

For more details, including technical use cases, Program qualification criteria and participant enrollment processes, please refer to the *Visa Delegated Authentication Program Implementation Guide*.

## 3.8 Visa Pre-dispute products



### 3.8.1 The benefits of reducing fraud rates attributable to unrecognized transactions and first party fraud

Disputes are often marked as fraud even when they are raised only because customers have trouble recognizing transactions and not because the transaction was unauthorised. Visa analysis indicates that fraud is reported 90% of the time a dispute is submitted.

Such disputes can artificially and unnecessarily inflate fraud counts, limiting the ability of Acquirers and Issuers to apply the TRA exemption and potentially limiting the ability of individual merchants to be considered for the application of certain exemptions.

Visa's experience has shown that a significant proportion of both disputes and transactions unnecessarily categorised as fraudulent can be avoided if customers and Issuers can be provided with additional information, such as the item purchased, to help customers validate transactions before they formally ask for a transaction to be disputed.

If merchants provide this information to Issuers it enables them to deal more effectively with customer queries, improving customer satisfaction and removing these transactions from the fraud count. This can potentially improve the risk score of every transaction a merchant processes, while increasing the ability of Acquirers and Issuers to apply the TRA exemption. Merchants can also benefit by reducing revenue losses from disputes, as well as increasing their ability to qualify for the application of key exemptions.

Verifi, a Visa company, offers a suite of related Pre-dispute Products to help both merchants and Issuers avoid and resolve such disputes.

### 3.8.2 Introduction to Verifi pre-dispute services

Verifi pre-dispute solutions provide an opportunity for merchants, Acquirers and Issuers to collaborate and share data to prevent and resolve disputes at the pre-dispute stage.

#### 3.8.2.1 Verifi Order Insight

Verifi's Order Insight® (formerly Visa Merchant Purchase Inquiry) allows merchants to share order details with Issuers through the existing Visa Resolve Online (VROL) dispute process. Enhanced transaction data is provided by merchants to Issuers for review with cardholders at first inquiry.

An overview of the Verifi Order Insight process is shown in Figure 15 below:

All Visa Issuers have real-time access to enhanced transaction details from enrolled merchants through VROL. In order to benefit directly, merchants need to enroll directly or via their Acquirer or payment facilitator.

#### 3.8.2.2 Order Insight Digital

Order Insight Digital (formerly Visa Cardholder Purchase Inquiry) enables cardholders to access the same enhanced transaction data through an Issuer's online banking portal or mobile app. Validating the sale with the cardholder can help prevent a dispute from being raised. Global Visa Issuers are required to receive transaction data in VROL from participating merchants before submitting a dispute.

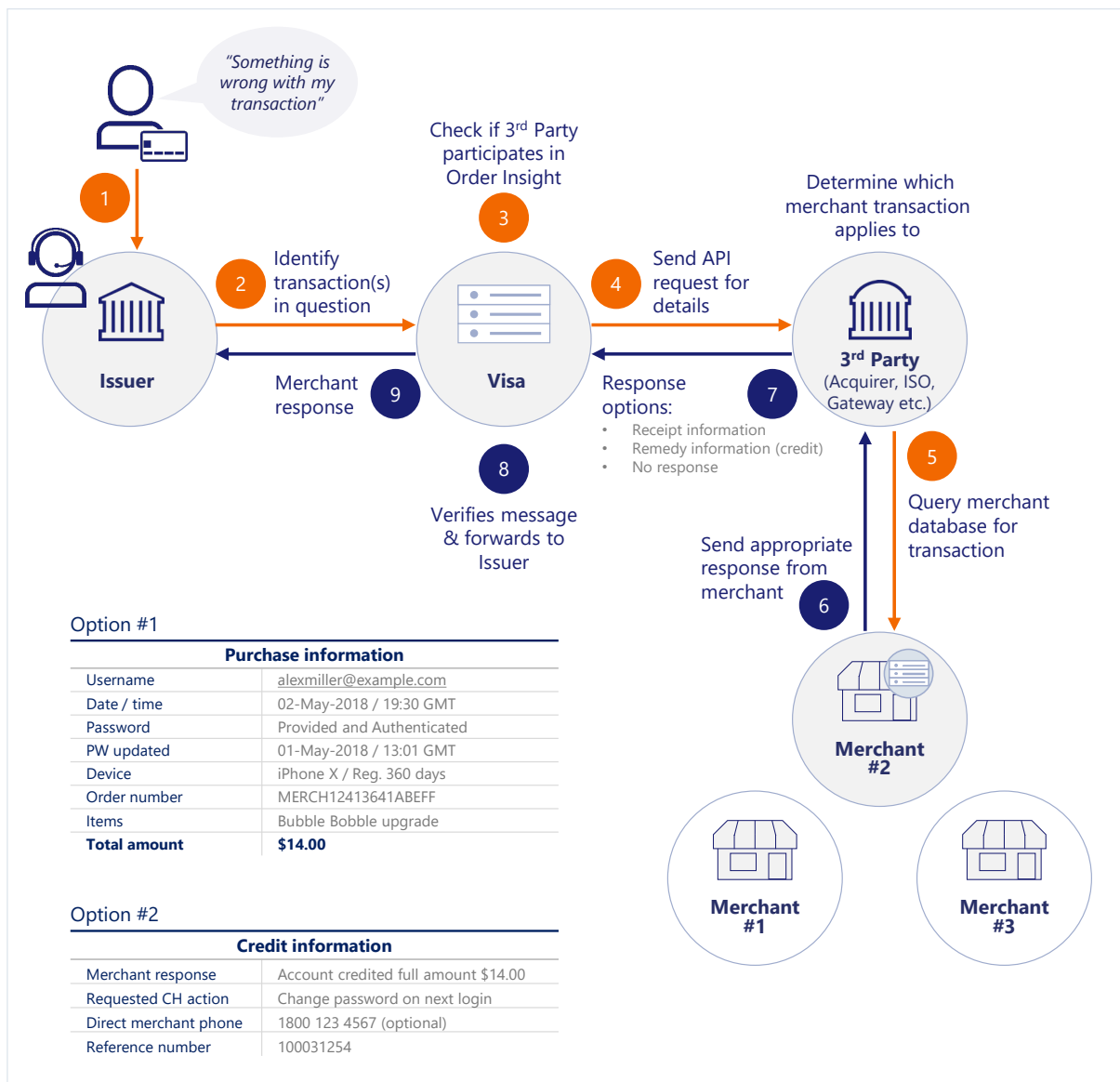
### 3.8.2.3 Rapid Dispute Resolution

Rapid Dispute Resolution (RDR) operates at the pre-dispute stage to resolve disputes before they escalate, as determined by seller-defined rules in the Verifi automated decisioning engine. Pre-disputes from other card brands can also be resolved through Verifi.

### 3.8.3 Accessing Verifi pre-dispute services

All Verifi services are available through VROL for Issuers, or through enrolment directly with Verifi for merchants. Interested parties should contact Verifi (info@verifi.com), or speak to their Visa representative. Small to medium Merchants should speak to their Acquirer about availability of these services.

Figure 15: The Order Insight process flow



## 3.9 The Visa MIT Framework



### 3.9.1 Introduction to the MIT Framework

#### 3.9.1.1 The requirement to use the MIT Framework in the context of PSD2

The Visa MIT Framework enables Acquirers and Issuers to correctly flag and identify MIT transactions.

#### Requirement

Merchants must use the MIT framework for any MITs if they want those transactions to be recognized as out of scope of SCA.

The Visa MIT framework was first introduced in 2016 and is a global standard to identify MITs, which, as payee initiated transactions, are out of scope of the PSD2 regulation.

The Visa MIT framework is not mandated to be used by merchants for PAN based transactions<sup>41</sup> (it is mandated for token based transactions). However, in the PSD2 context, if the framework is not used, the Issuer will not be able to recognize an MIT as out of scope of PSD2 and may unnecessarily decline, requesting SCA even though the cardholder is not available. To avoid this experience, the MIT Framework needs to be implemented by the ecosystem for all MITs, PAN or token based.

#### 3.9.1.2 Types of MITs defined within the Visa MIT Framework

The Visa MIT framework defines eight distinct types of MITs as summarized in Table 14 below and identifies each of these using two distinct identifiers:

- **Transaction type:** Located in Field 126.13 (POS Environment Code Field) or Field 63.3 (Message Reason Code Field), depending on the transaction intent of the MIT.
- **Transaction identifier (Tran ID) of the initial CIT<sup>42</sup>:** Located in Field 125, Usage 2, Dataset ID 03

For more details see Table 15 below.

<sup>41</sup> Not mandated by Visa for merchant to use for PAN based transaction, however all Acquirers were mandated to be ready to support it since October 2017 for all transactions (PAN and token) and all Issuers were mandated to be ready to receive MIT indicators since 2016 for all PAN and token based transactions.

<sup>42</sup> Or of the previous MIT in some cases as indicated in Table 20.

**Table 14: 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, 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 transaction 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 are 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. 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>An incremental authorization can also be used in Europe to authorize any additional amount above the authenticated amount when the price of merchandise or services, including shipping costs and applicable taxes has changed, so long as the cardholder has entered an agreement in advance to pay the additional amount.</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. This is only applicable to contactless transit transactions.</p>

**Table 15: Key data fields of the Visa MIT Framework**

MIT TYPE Description	Visa MIT Framework		
	POS environment (F126.13)	Message Reason Code (F63.3)	Transaction ID (F125 <sup>43</sup> )
Installment/Prepayment	I	--	Tran ID of first transaction (CIT)/ previous MIT
Recurring	R	--	Tran ID of first transaction (CIT)/ previous MIT
Unscheduled Credential on File (UCOF)	C	--	Tran ID of first transaction (CIT)/ previous MIT
Incremental	--	3900	Tran ID of first transaction (CIT)
Delayed Charges	--	3902	Tran ID of first transaction (CIT)
No Show	--	3904	Tran ID of first transaction (CIT)
Reauthorization	--	3903	Tran ID of first transaction
Resubmission	--	3901	Tran ID of first transaction

### 3.9.1.3 MITs qualifying as out of scope of SCA

An MIT is 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.

It is the Acquirer’s responsibility to ensure that transactions indicated as MITs meet all the requirements in this section. In the EEA and the UK, a merchant can only submit a transaction indicated as an MIT with the Visa MIT Framework if the transaction meets all of the requirements of an MIT as defined in this section, including:

<sup>43</sup> Acquirers may submit the Original Transaction Identifier either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Transaction Identifier in Field 125 to the Issuers that participate to receive Field 125.

- The cardholder must not be available to (I) initiate; or (II) authenticate the transaction. If the cardholder is available to do either of those things, then the transaction is not an MIT.
- SCA must be applied (exemptions cannot be used) to the initial Customer Initiated Transaction (CIT) used to establish the agreement for future MITs. This applies if the agreement was set up through a remote channel<sup>44</sup>, unless the initial CIT:
  - Was performed prior to the enforcement date<sup>45</sup>
  - Is out of scope of SCA e.g. MOTO.

Where these requirements are met, an MIT does not require SCA. However, SCA must be applied when certain changes are made to the agreement, for example if the cardholder wishes to use a different card. For merchant driven changes to payment terms, such as payee changes to price due to inflation, 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.

Additionally, there is no need for SCA to have been applied to the initial CIT used to establish the agreement for future MITs in the following scenarios:

- The transaction qualifies for the secure corporate payments exemption
- The Transaction is a Resubmission or Reauthorization, as defined under the Visa MIT framework, and is simply the completion of an existing CIT (i.e. it is not an MIT for regulatory purposes). The CIT will have been authenticated, or qualified for an exemption, when it was originally initiated by the cardholder.

An MIT can only be submitted where it is subject to a specific agreement set up with the cardholder as part of the initial CIT and clearly disclosed to that cardholder. The agreement should clearly define the circumstances under which an MIT may be used, including, but not limited to, the following<sup>46</sup>:

- Name and full address of Merchant
- Purpose of the agreement / payment
- Type of payment (such as recurring, no show, prepayment)
- Timing and frequency of the transaction or the event that will trigger the transaction
- The transaction currency and amount or a description of how the transaction amount will be determined

---

<sup>44</sup> PSD2 specifically states that SCA applies to payments initiated by the payer. The EBA and FCA have confirmed that transactions initiated by the payee are out of scope of SCA as long as SCA was applied when setting up the mandate if that mandate was set up via a remote channel and there is a risk of fraud or other abuses. In Visa's view, SCA is also required whenever an MIT mandate is set up via a face to face transaction – exemptions cannot be applied.

<sup>45</sup> Merchants, Acquirers and Issuers should note that enforcement dates may differ between markets as determined by local NCA's. This is currently 31 December 2020 for most of the EEA, and 14 September 2021 for the UK.

<sup>46</sup> Refer to the Visa rules for specific required T&Cs for different transaction types (for example for guaranteed reservations).



- Total amount and currency of the agreement (or if final amount is not known, details on how the final amount will be calculated)
- Amount and currency of the authentication
- Cancellation procedure
- Additional T&C clauses may be required based on the nature of the transaction, including potential expiration date
- The merchant must also provide a copy of the MIT agreement with the consumer via email

In addition to MITs that are out of scope, the MIT framework will also flag some transactions which are not out of scope but where SCA has already been performed or an exemption has been applied before the transaction is executed.

This is the case for the following types of MITs from the Visa MIT Framework because in these cases the transactions are simply the completion of an existing transaction where SCA was already performed (or the transaction was exempt), and so no further authentication of the cardholder is required. The CIT does not require SCA if an exemption is applicable, even if the transaction may be subsequently completed with the MIT indicator.

- *Resubmission*: This is the case for a contactless transit transaction where an exemption applied. The transaction may have been initially declined due to insufficient funds, but as the service was already rendered, it is permitted by Visa Rules to be resubmitted for completion.
- *Reauthorization* (used in delayed or split authorizations): this is the case where the merchant is permitted or required to either repeat or split an authorization in order to complete an existing payer initiated transaction under Visa Rules (e.g. because the original authorization has expired, or because the order cannot be delivered in one shipment).

This is also the case when:

- A cardholder agrees to pay a No Show fee with an eligible merchant and the agreement is made during a booking made via a secure corporate payment process that qualifies for application of the secure corporate payments processes and protocols exemption. In Visa's view, it is permissible that SCA is not performed on the CIT that sets up the No Show agreement providing that the secure corporate payments exemption is applicable, and the PSP considers there is no risk of fraud<sup>47</sup>.
- An MIT is set up via MOTO as MOTO transactions are out of scope of SCA.

### Requirement

The initial CIT used to establish an agreement for future MITs is in scope of SCA, and it is required that SCA is applied in most cases (for exceptions see above), For more details on how to establish an agreement, refer to Section 5.11 of version 2.0 of this guide.

<sup>47</sup> For example use cases please Sections 5.11.1 and 5.17 in version 2.0 of this guide.

### 3.9.2 Acquirer use of the Visa MIT Framework



To avoid inadvertent declines, it is essential that Acquirers / merchants use the existing Visa MIT Framework to enable Issuers to properly identify transactions which are out-of-scope MITs and where the Issuer should not request SCA. It is their responsibility to ensure that any transactions they indicate as MITs are legitimate MITs, as per the criteria listed above.

#### 3.9.2.1 Populating the original Transaction ID for MITs

The Visa MIT framework requires that an Acquirer includes a transaction ID relating to previous relevant transaction in Field 125 or 62.2 as follows:

- For recurring, installment and unscheduled COF transactions, Visa MIT framework processing requirements allow Acquirers to use either the initial CIT or previous MIT Transaction ID. In Europe, Visa recommends using the initial Transaction ID to link to the transaction where the mandate to process MITs was set up.
- For Incremental, No Shows, Delayed Charges, Resubmission and Reauthorization, the Transaction ID of the initial CIT must be used.

#### 3.9.2.2 Grandfathering

For MITs covered by cardholder agreements that were established prior to the regulatory enforcement date, those transactions should be able to continue to be processed without SCA as long as they are identified as MITs using the Visa MIT Framework. If the transaction ID of the initial transaction where the mandate was set up is not available, the transaction ID of any related MIT processed before the regulatory enforcement date can be used. Visa recommends that clients store the transaction ID of the selected transaction and include it in future related MITs to represent the "initial" transaction. However, as stated above, the transaction ID of the previous MIT is also acceptable to use for recurring, installment and unscheduled COF transactions.

#### 3.9.2.3 Visa provided interim Tran IDs

Visa is aware that enhanced system development may be required to store Tran IDs of previous transactions. Accordingly, to assist with merchant readiness in time for the regulatory enforcement date, if the merchant is unable to obtain an initial or previous transaction ID to pass on to the Acquirer, Visa will provide Acquirers, on request, a Visa Acquirer-assigned interim Tran ID for use in place of a valid Original Tran ID on an interim basis. This interim identifier can be used by any merchant acquired in the EEA providing its Acquirer supports this feature. This will give the Acquirer and the merchant additional time to make the necessary system changes. The Acquirer should contact their client service representative to obtain this interim Tran ID<sup>48</sup>.

Acquirers who are using an interim Tran ID should refer to waiver letters from Visa for the final date by which they must stop using the interim Tran ID and ensure that merchants using them are aware of the final date.

---

<sup>48</sup> Refer to Article 2.17 of the *October 2019 and January 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 5 September 2019* for more details.

Merchants using an interim Tran ID (or their gateway provider or Acquirer) must, prior to the final date, be in a position to store a valid Tran ID of an MIT that was populated with the interim identifier and successfully approved. This will enable the merchant to start using a valid Tran ID instead of the interim one for MITs initiated after the final date of usage of the interim Tran ID.

Merchants using an interim Tran ID for annual subscriptions should take particular care to ensure that they have obtained a valid Tran ID sufficiently well in advance of the expiry of the interim Tran ID. This is necessary to ensure they are able to process subscription payments due after the final date.

Table 17 provides a view of the impact of using this Visa Acquirer-assigned interim Tran ID.

#### 3.9.2.4 Populating the POS entry mode for MITs

Note that while the POS entry mode field (Field 22) is not part of the MIT Framework, it is important it is populated appropriately as presented in Table 16.

- Note that for any of the transactions in Table 16, be they first (CIT) or subsequent transactions (MITs), the merchant should use POS entry mode 10 (which means “stored credentials”) for the transaction if it is performed using an existing stored credential. As Recurring, Installment, or UCOF MITs can only be performed when credentials are stored, those MITs always require the use of POS Entry Mode 10.
- However, Incremental, No Shows, Delayed Charges, Reauthorization, or Resubmission MITs should only use POS entry mode 10 if the merchant stored the payment credentials for future purchases as part of an agreement with the customer. POS entry mode 10 should not be used if the credential is only stored to complete this specific transaction. For more information about the Stored Credential Framework and what is required to use it, see Appendix A.1.

### 3.9.3 How Issuers identify MITs



Issuers must be able to recognize MITs to avoid requesting SCA which cannot be performed due to cardholders not being available to authenticate the transaction. They can do so using one of the following ways:

- Using the Visa MIT Framework, (see Table 15), or
- The initiating party indicator introduced in Field 34 (see Table 16), as documented in *Article 9.1.4 of the October 2019 and January 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 5 September 2019*.

Whichever method is used to identify an MIT, Issuers may not use an SCA decline code in response to an authorization request for a properly identified MIT, to avoid any associated friction and inadvertent declines due to the cardholder not being available for authentication.

#### 3.9.3.1 Issuer identification of MITs using the new value in Field 34



Visa is introducing a new indicator for Issuers to identify an MIT as out of scope of SCA. The indicator is in Field 34 (Tag 80, Dataset ID 02) i.e. the same field Issuers use to check for exemptions to SCA.

The Acquirer must continue to use the existing Visa MIT Framework to indicate MITs. When receiving transactions that are indicated as MITs using the framework, Visa will automatically populate the value of "1" in Field 34 (Tag 80, Dataset ID 02), as depicted in Table 16. This enables Issuers to recognize a transaction as a MIT out of scope in real time by simply looking for the value of "1" in that tag. Visa does not validate whether the initial CIT referenced with the MIT was authenticated. However Acquirers are required to ensure a transaction flagged as an MIT meets all requirements, including authentication at set-up. Issuers using this method at time of authorization may wish to receive and store the Tran ID populated in F125 for every MIT to provide an audit trail in case they are ever required to prove that authentication took place at MIT set up.

### 3.9.3.2 Issuer identification of MITs using the Visa MIT Framework



The Issuer can alternatively recognize an MIT using the existing Visa MIT framework. This is done by looking for the presence of the MIT type identifier in Field 126.13 or F63.3 and the Tran ID of the initial CIT (or previous MIT in some cases) in Field 125.

Only Issuers that are enabled to receive Field125 will get this value. Issuers must check with their account executive/customer support regarding how they can technically enable their system to receive Field 125.

Issuers that choose to use the existing Visa MIT Framework to identify these transactions as out of scope of PSD2 / SCA requirements must be aware that:

- The number populated in Field 125, Usage 2, Dataset ID 03 represents the Tran ID of the initial CIT or of a previous MIT transaction. However, Visa has assigned Tran IDs to Acquirers for use in this field and will continue to do so for an interim period of time. Therefore, in those cases, Issuers will see a value of "0100000000000000" in Field 125<sup>49</sup>, indicating that the merchant/Acquirer was not ready to send a valid Tran ID for this MIT. Issuers are asked to accept this value for an interim period of time.
- The transaction ID the Issuer will see in F125 of an MIT will therefore be one of the following:
  - The valid Tran ID of a valid initial CIT or previous MIT
    - This includes the Tran ID of a previous MIT processed with the interim identifier of "0100000000000000" which is the case when a merchant that was initially not ready (and was thus using an Acquirer assigned Tran ID) starts to use a valid Tran ID of a previous MIT.

Or:

- The interim Issuer transaction id of "0100000000000000"<sup>49</sup>

---

<sup>49</sup> This is with effect from 31 August 2019. Prior to that date, the Issuer would simply see another value (which may differ per Acquirer) assigned by Visa to the Acquirer but not representing a valid transaction identifier of a transaction previously processed with this card and Issuer. For further details, refer to Article 2.17 of the *October 2019 and January 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 5 September 2019*.

- This is the case when a merchant was not ready to send a real Tran ID but did send one assigned to them by Visa for this purpose
- This can represent a MIT that is being grandfathered, or an MIT put in place after 14 September (with SCA applied) but where the merchant is still not ready to send a valid Tran ID
- For transactions indicated as recurring, installment or unscheduled credential on file (UCOF) by a value in Field 126.13, these can be either customer-initiated or merchant-initiated. It is the presence of a value in Field 125, Usage 2, Dataset ID 03, which will allow Issuers to identify these transactions as MITs: a CIT, unlike an MIT, will carry no value in Field 125. The value "10" in Field 22 (POS Entry Mode) indicating the transaction is performed with stored credential does not necessarily indicate that a transaction is a MIT, as it may also be present in a CIT.

Please refer to Table 16 to identify all the key data fields and values to be used in authorizations to identify CITs used to set up MIT agreements and MITs.

**Table 16: Key data fields and values for MIT transactions and CITs used to set up MIT Agreements**

Description	Transaction Type	Visa MIT Framework			POS Entry Mode (PEM) (F22)	Initiating Party Indicator (F 34 <sup>i</sup> )	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125 <sup>ii</sup> )			
Installment/ Prepayment	First Transaction (CIT)  (May be of zero value if set up only)	I	--	--	Any valid <sup>iii</sup> (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	I	--	Tran ID of first transaction/ previous MIT  (or interim Tran ID)	10	1 <sup>i</sup>	N/A
Recurring	First Transaction (CIT)  (May be of zero value if set up only)	R	--	--	Any valid <sup>iii</sup> (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	R	--	Tran ID of first transaction/ previous MIT  (or interim Tran ID)	10	1 <sup>i</sup>	N/A

Unscheduled Credential on File (UCOF)	First Transaction (CIT) (May be of zero value if set up only)	C	--	--	Any valid <sup>iii</sup> (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	C	--	Tran ID of first transaction/ previous MIT <i>(or interim Tran ID)</i>	10	1 <sup>i</sup>	N/A
Incremental	First Transaction (CIT) (Estimated transaction)	--	--	--	Any valid <sup>iii</sup> (10 if stored credential)	--	Required
Incremental	Subsequent Transactions (MIT)	--	3900	Tran ID of first transaction	Any valid <sup>iii</sup> (10 if stored credential)	1 <sup>i</sup>	N/A
Delayed Charges	First Transaction (CIT)	--	--	--	Any valid <sup>iii</sup> (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	--	3902	Tran ID of first transaction <i>(or interim Tran ID)</i>	01 or 10 if stored credential	1 <sup>i</sup>	N/A
No Show	First Transaction (CIT)	--	--	--	Any valid <sup>iii</sup> (10 if stored credential)	--	Required (except if secure corporate payment exemption applies)
	Subsequent Transactions (MIT)	--	3904	Tran ID of first transaction <i>(or interim Tran ID)</i>	01 or 10 if stored credential	1 <sup>i</sup>	N/A
Reauthorization	First Transaction (CIT)	--	--	--	Any valid <sup>iii</sup> (10 if stored credential)	--	Exemption may be used. <sup>v</sup> If CAVV available, may or may not

							be present as the merchant has the option to provide in the initial CIT or in the MIT reauthorization
	Subsequent Transactions (MIT)	--	3903	Tran ID of first transaction (or interim Tran ID)	01 or 10 if stored credential		Not required but CAVV may optionally be present
Resubmission	First Transaction (CIT)	--	--	--	Any valid <sup>iii</sup> (10 if stored credential)	--	Contactless exemption applies <sup>v</sup>
	Subsequent Transactions (MIT)	--	3901	Tran ID of first transaction (or interim Tran ID)	01 or 10 if stored credential	1 <sup>i</sup>	N/A

Notes:

- i. The new initiating party indicator indicates a transaction is an MIT out of scope of SCA indicator and is populated in Field 34 Tag 80 and is for Issuer use only. Visa will automatically populate the value 1 in Field 34 Tag 80 for Issuer usage when a transaction is submitted by an Acquirer using the existing Visa MIT Framework.
- ii. Acquirers may submit the Original Tran ID either in Field 62.2 or in Field 125 Usage 2 DS 03. Visa then forwards this Original Tran ID in Field 125 to the Issuers that participate to receive Field 125. The Transaction ID in F62.2 which is presented in the authorization request to Issuers and response back to Acquirers is the one of the current MIT and not that of the initial CIT as Visa always generates a new, unique, Tran ID for each transaction, including subsequent MITs, in this field (except in the case of incremental authorizations where the initial Tran ID is kept).
- iii. Any valid value because these transactions can also originate in F2F channels.
- iv. Incremental transactions must be preceded by an estimated/initial authorization. The estimated authorization indicator with a value of 2 or 3 must be included in Field 60.10 - Additional Authorization Indicators.
- v. The associated subsequent MITs are simply the completion of an existing transaction, no further authentication of the cardholder is required as long as the CIT was compliant, i.e. if exemptions were applicable, they can be used.

Refer to Table 17 for a visual representation of the impact of the usage of interim Tran IDs in MITs, both from an Issuer and Acquirer perspective.

**Table 17: Acquirer and Issuer View of MIT Transactions with usage of Visa assigned interim Tran IDs**

CIT Types	Visa Existing MIT Framework – Acquirer View <sup>50</sup>			MITs – Issuer View			
	POS Env. (F126.13)	Reason Code (F63.3)	Field 125 or F62.2	POS Env. (F126.13)	Reason Code (F63.3)	Field 125	Initiating Party Indicator (F 34, Tag 80 Dataset 02 <sup>51</sup> )
Standing Instruction MITs (Recurring, Installments/ Prepayments & UCOF)	R, I or C	-	Tran ID of initial CIT or previous MIT	R, I or C	-	Tran ID of initial CIT or previous MIT	1
	R, I or C	-	Visa Acquirer assigned Interim ID	R, I or C	-	01000000 00000000	1
Industry Specific MITs – except Incrementals (Resubmission, Delayed Charges, Reauthorization, No Show)	-	3901 to 3904	Tran ID of initial CIT	-	3901 to 3904	Tran ID of initial CIT	1
	-	3901 to 3904	Visa Acquirer assigned Interim ID	-	3901 to 3904	01000000 00000000	1
Incrementals <sup>52</sup>	-	3900	Tran ID of initial CIT	-	3900	Tran ID of initial CIT	1

<sup>50</sup> It is the Acquirer’s responsibility to ensure that any transactions they indicate as MITs meet the requirements defining an MIT. Acquirers may also use the Visa MIT Framework to indicate some transactions that are in scope but where SCA was performed or an exemption applied, notably in the cases of resubmitted transit transactions (resubmission MIT type) or delayed or split authorizations (reauthorization MIT type).

<sup>51</sup> When Visa receives a transaction indicated as an MIT, it will automatically populate the value of “1” MIT out of scope of SCA in F34.

<sup>52</sup> An Acquirer assigned transaction identifier must not be used on incremental transactions.



### 3.10 Visa Biometrics



Visa has designed various products and services to help our clients to utilize biometrics to authenticate customers.

For clients that need support in getting started with the technology, Visa has a discovery program that explores various biometrics technologies available, helps clients to test the user experience and understand security, risks and implementation considerations.

Visa provides an easy to implement authenticator app for clients who use Visa Customer Authentication Service (VCAS) and are looking to launch an app plus biometric solution with minimum deployment of internal resources. The app can be Issuer branded and launched in a short timescale. It also supports other authentication use cases such as account recovery and remote customer verification for call centres.

Please contact your Visa representative if you would like more information on VCAS and Visa's authenticator app solution.

### 3.11 Visa Consumer Authentication Service



Visa Consumer Authentication Service (VCAS) is a data-driven hosted ACS solution designed to support an Issuer's authentication strategies delivered through 3-D Secure.

At the core of the product are Risk Based Authentication (RBA) capabilities, which work behind the scenes to evaluate each transaction based on data exchanged between the merchant, the Issuer and Visa. This can help to considerably reduce friction during checkout, whilst also providing greater levels of security. To deliver this, VCAS assesses the risk of a transaction in real-time using predictive risk analysis based on a number of enhanced inputs, including device and transaction information and behaviors. This network-wide level of intelligence gives Issuers more information to decide if and when additional authentication is needed.

The VCAS Compliance Manager application provides Issuers with insight into what transactions may need SCA, identifies transactions that may qualify for exemptions, may help prevent collision between compliance and risk rules and also gives an Issuer the flexibility to override exemptions with additional rules. Issuers will maintain control over whether they approve transactions. When SCA is required, VCAS supports multiple methods for Issuers to perform SCA, including biometrics, one-time passcodes and push notifications to the Issuer's Mobile Banking App.

The VCAS Portal gives Issuers unprecedented flexibility to refine risk strategies through custom rules based on multiple parameters and to anticipate or respond to new fraud trends as they emerge.

The VCAS solution has been built in partnership with CardinalCommerce, an industry leader in digital payment authentication that is fully owned by Visa. VCAS will fully support 3DS 1.0 and EMV 3DS along with the other authentication products in the Visa portfolio. Issuers seeking support in migrating to EMV 3DS may wish to consider VCAS as an option to enable the transition.

For more information please see <https://www.cardinalcommerce.com/products/visa-consumer-authentication-service>.

# 4. Optimizing the payment experience under PSD2

## 4.1 Introduction



Under PSD2, SCA is not required for all electronic transactions. Some transactions are out of scope of the regulation or exempt and where this is the case, SCA is optional and in some cases should not be used.

Clients will need to assess and decide how to treat each transaction with regards to the application of SCA based upon a combination of factors including:

- Whether a transaction is out of scope or qualifies for an exemption
- Fraud risk
- Optimization of user experience
- Liability protection

It is critical that merchants and Acquirers flag transactions correctly to ensure Issuers are able to identify transactions where SCA is not needed and authorize appropriately.

Merchants and Acquirers who wish to request or apply an exemption should only apply or request one exemption per transaction by setting one exemption indicator in the appropriate EMV 3DS and/or authorization request fields.

Visa provides a number of tools and services (described in Section 3) to enable clients to take full advantage of the application of exemptions while keeping fraud rates low.

This Section 4 provides guidance on:

- Key principles that clients should apply when assessing, routing, flagging and processing transactions
- The main decision points in a basic transaction flow for both merchants/Acquirers and Issuers and on the assessment and treatment of a transaction at each point
- Use of the MIT framework for managing out of scope Merchant Initiated Transactions
- Practical application of the main exemptions (building on previous sections)
- Issuer deployment of EMV 3DS including selection of challenge methods and optimization of user experience
- Issuer processing
- 3DS and authorization fall back options (The Visa Attempts Server and STIP)
- The application of SCA in the context of Visa Direct transactions

More detailed guidance on the application of SCA, authentication and authorization flows for specific transaction use cases is included in section 5 of version 2.0 of this guide, however

please also read summary guidance provided in section 5 of this version 3.0 before referring to version 2.0.

## 4.2 Key principles

### 4.2.1 Transactions that may be submitted for Authentication or direct to Authorization



Transactions that are out of scope or qualify for an Acquirer exemption may be submitted for authentication or sent directly to authorization, with the appropriate indicators as described in section 3.2.9.

Factors to consider when selecting the appropriate option are summarized in section 4.3.

### 4.2.2 Managing variations in amount & merchant name



#### 4.2.2.1 The regulatory requirement

The PSD2 SCA dynamic linking requirement, which is summarised in section 2.4 requires that (i) the payer is made aware of the amount of the payment transaction and of the payee; that (ii) 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 (iii) any change to the amount or the payee results in the invalidation of the authentication code generated.

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. For more information on the use of the CAVV and TAVV please see section 3.2.7.

There will be legitimate scenarios where there is not an exact match between the merchant names and amounts submitted during authentication and authorization and Issuers should not decline transactions just because there is not an exact match, provided the final amount does not exceed the authenticated amount and that any name variations are legitimate. The following sections expand on these points.

#### 4.2.2.2 Managing variations in merchant name

As described in section 2.4, the payee information included in the authentication code may not necessarily need to be the full or exact merchant name, but can match a unique identifier corresponding to the payee at authentication.

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 recognizable 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.

#### 4.2.2.3 Managing variations in amount

As described in section 2.4, the EBA has confirmed that the final amount should not increase above the authenticated amount. 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.

To address use cases where the final amount is higher than the authenticated amount, with the publication of the October 2020 Visa Rules<sup>53</sup>, Visa removed existing authorization tolerance limits and expanded the availability of its existing estimated / incremental authorization framework to additional merchant segments for EEA transactions by:

- Eliminating existing authorization tolerance limits that allow e-commerce and tipping merchants to clear an amount greater than the authorized amount
- Allowing all e-commerce merchants in the EEA to use initial / estimated and incremental authorizations in the event that the final transaction amount is anticipated to differ from the initial authorized and authenticated amount (Visa Rules ID#: 0025596)

For transactions in the UK, at the time of writing, discussions are underway with the UK Financial Conduct Authority regarding the allowance of a reasonable variation to authorization amounts. Until discussions conclude, Visa will not prevent UK merchants from continuing to clear up to 15% greater than they authorized / authenticated (although Issuers and Acquirers will need to make their own decisions regarding such transactions). However, as of 17 October 2020, all UK e-commerce merchants are permitted the same flexibility as EEA merchants to use initial / estimated and incremental authorizations.

Use cases where the final amount may increase after authentication<sup>54</sup> are provided below.

#### 4.2.2.3.1 Options for handling amount variation due to changes not initiated by the customer

There are several use cases where the final amount the customer should be charged for is not known at checkout and can end up being higher than the amount authenticated due to circumstances after checkout that are not initiated by the cardholder. Examples include:

- Purchases where final shipping costs and/or taxes are not known at the time the customer checks out and authenticates
- Online grocery shopping, where the actual cost of weighed goods is not known until the order is picked or when pre-agreed substitutions are made for ordered goods that are unavailable.

In such cases the final amount cannot be calculated until the fulfillment process is complete and/or the order is prepared for dispatch at which time the cardholder is no longer available for reauthentication.

Merchants have two options for dealing with such cases. They should consider the technical, operational and customer experience impacts of each option.

---

<sup>53</sup> For details, please refer to *Visa Business News Expanded Eligibility for Estimated and Incremental Authorization in the EEA and UK to Support Amount Variation*, (AI106007).

<sup>54</sup> Recurring payments and unscheduled card-on-file transactions are MITs and therefore are not impacted. Amounts can vary in line with the terms and conditions agreed upon with the customer for those transactions.

### Option 1—Merchant-initiated transaction (MIT) incremental authorization:

This is the Visa-preferred option from a customer experience perspective.

When a merchant knows that a finmount may vary when the cardholder is no longer available to authenticate, they process the initial authorization with the “known” amount at checkout as an “initial or estimated”<sup>55</sup> amount and the additional unauthenticated authorization amount as an MIT—Incremental<sup>56</sup>. More specifically:

At the time of authentication:

- Terms and conditions specifying how the final amount will be calculated and when the charges will be collected must be disclosed and agreed to by the customer.
- Authentication is performed on a “known” initial amount with the application of an SCA challenge; no exemption can be used when setting up an agreement for the merchant to process a future MIT.

At the time of authorization:

- The authenticated amount is authorized as a CIT with the authentication data ECI values and CAVV and an “estimated authorization request indicator”<sup>57</sup> informing the Issuer that this is an estimated authorization that may be followed by an MIT—Incremental, if required.
- If the final amount is higher than the authenticated / authorized amount, the additional amount is authorized as an MIT—Incremental, which includes a reference to the initial CIT. 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. Depending on when the initial or estimated authorization takes place (which, dependent on business process, may be straight after authentication or at a later time), an MIT—Incremental may be submitted shortly after the initial or estimated authorization or later. Multiple additional incremental authorizations may also occur before the transaction is finalized for clearing and settlement.
- Note that if the final amount is lower than the authenticated / authorized amount, merchants must process partial reversals for the amount of the difference.

Clearing and settlement:

- When the final amount is cleared / settled, the cardholder will see a single transaction for the total amount on their bank statement / mobile banking transaction history.

---

<sup>55</sup> An amount is considered as “initial or estimated” in the authorization request due to the presence of the estimated indicator in the request. In this first option, it is recommended to use the “known” amount at the time of checkout as the “initial or estimated” amount. (The Visa Rules also allow for the use of an “estimated” amount prior to an MIT—Incremental, but in the context of PSD2 SCA, estimated amounts are recommended for use with option 2 rather than option 1).

<sup>56</sup> A transaction can only be processed as an MIT when the cardholder is not available to initiate or authenticate the transaction. If the cardholder is available to do either of these, the transaction cannot be processed as an MIT and option 2 must be considered instead.

<sup>57</sup> Merchants should contact their Acquirers for details of the rules associated with the use of initial or estimated authorizations and incremental transactions as well as appropriate flagging.

## Option 2—Perform initial authentication for a highest estimated amount:

An alternative method for handling potential amount variation, which may avoid requesting an authentication step-up, is to authenticate at checkout for the highest possible amount that would cover any anticipated amount variation. This option may, however, cause customer confusion or cart abandonment if the cardholder is unclear why they are being asked to authenticate for a higher amount than the checkout value of the goods or services. It is essential for merchants pursuing this option to clearly communicate to the customer (i.e., including prior to presentation of the EMV 3-D Secure challenge window if SCA is required) that:

- They are being authenticated for a maximum authorization amount.
- 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 (e.g., shipping and taxes).
- No charges will appear on their card statement until the order is finalized.

The final amount processed at the time of authorization can only be lower than or equal to the authenticated amount. If the final amount is higher, a new authentication will be required (i.e., the customer must be re-contacted if they are no longer available to authenticate).

If the final amount is lower, and the authorization has already been processed, a reversal must be processed for the difference.

Note that with this option, an SCA exemption may be applied at authentication as long as the transaction qualifies.

If the merchant considers that there is any possibility that the actual final amount will exceed the authenticated amount and does not want to have to re-contact the customer, option 1 should be selected.

### 4.2.2.3.2 Unplanned Higher Amount

In the event that the final amount is higher than the authenticated amount and the merchant had not planned for it using either of the options above, the merchant will need to contact the cardholder to authenticate the additional amount. The merchant then has the choice to:

- Authenticate for the new total final amount and submit one final authorization with this final amount (exemptions can be used if applicable), in which case, if an initial authorization had been processed prior to this, it must be reversed in full, or
- Authenticate only for the additional amount (exemptions can be used if applicable) and submit two authorizations, one for the initial amount and one for the additional amount, each with their respective authentication value or exemption indicators, as applicable.

An additional amount cannot simply be processed by the merchant as an additional authorization with an exemption indicator: even if a transaction for this amount would qualify for an exemption. The customer must initiate new transaction. This is the case because if the transaction is initiated by the merchant it would be an MIT, which cannot be processed without prior customer consent and authentication. Exemptions can only be applied to customer initiated transactions.

#### 4.2.2.3.3 Amount variation due to a customer adding to a basket

In some use cases, a customer 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. For example, an online grocery shopping service or a food delivery service may allow customers to checkout and authenticate to secure their delivery slot and then change items in their basket until a cut-off time a set number of hours before delivery. In this case, the final amount would be calculated, and the authorization submitted after the cut-off time when the customer is no longer available to authenticate. A customer making several incremental changes to an order in this way may not know which will be their final change that determines the final amount of the order. In this case, the following two options are available.<sup>58</sup>

##### **Option 1 - Re-authenticate every time the cardholder adds to the basket**

Authentication is performed for the new total amount every time the customer edits the order. If the transaction qualifies for an exemption, SCA challenges do not need to be applied, and the customer experience may be frictionless. In this case authentication should be requested through EMV 3DS with an appropriate exemption indicator.<sup>59</sup>

This option may be appropriate in cases where there is a high likelihood of qualification for an exemption, for example if the merchant is enrolled in Visa Trusted Listing and the customer has added the merchant to their Trusted List or when the expected value of the basket is such that the transaction should qualify for the Acquirer TRA exemption. Merchants should however be aware that an Issuer may choose to apply an SCA challenge, e.g. if it considers the transaction to be high risk.

##### **Option 2 - Authenticate at checkout for a highest estimated amount**

The merchant can authenticate at initial checkout for a maximum estimated amount that would cover potential additions to the basket. Whenever the customer edits the basket, no further authentication is required as long as the new total amount is below or equal to the authenticated amount. If a change increases the total amount above the authenticated amount, a new authentication must be performed for the new total amount. Qualifying exemptions may be applied as described in the previous option.

This option may be appropriate in cases where a transaction is less likely to qualify for an exemption. However, it may cause customer confusion/cart abandonment at authentication if the cardholder is unclear as to why they are being asked to authenticate for a higher amount than the checkout value of the goods or services ordered. If this option is selected it is essential to clearly communicate to the customer prior to authentication (i.e. prior to the presentation of the 3DS challenge window) that:

- They are being authenticated for an estimated maximum amount

---

<sup>58</sup> For both option 1 and 2, remember however that if at fulfilment the amount varies due to circumstances not initiated by the cardholder, the authorization cannot be processed for a higher amount than what was authenticated. See procedures described for those scenarios in section 4.2.2.3.1.

<sup>59</sup> If the exemption is only requested later at time of authorization and declined, the cardholder will no longer be available for authentication, therefore the exemption request is best handled via EMV 3DS.

- 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 (e.g. shipping and taxes)
- No charges will appear on their card statement until the order is finalised

#### 4.2.3 MITs, CITs, stored credentials and account verification transactions



In order to understand how to manage MITs in a PSD2 environment it is important to be familiar with some key concepts:

- **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 subsequent payments from the card without any direct involvement of the cardholder. As the cardholder is not present when an MIT is performed, cardholder authentication is not possible. A transaction can only be an MIT if the user is not available to (I) initiate; or (II) authenticate. If they are available to do either of those things, then it is not an MIT. See section 3.9.1.3 for a full definition of an MIT.
- **A cardholder-initiated transaction (CIT)** is any transaction that is not an MIT as defined in section 3.9.1.3, and includes any transaction where the cardholder is available to initiate or authenticate the transaction. Authentication is required for all CITs, unless the transaction qualifies for an exemption or is otherwise out of scope of SCA.
- **A stored credential** is 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. Visa has introduced a Stored Credential Framework to govern the use of stored credentials. More details are included in Appendix A.1. 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.
- **Account verification transactions** are authorization requests initiated by merchants for zero value in order to verify a cardholder’s account. Whether an account verification transaction requires SCA or not depends on the use case. Descriptions of use cases and when SCA is required are given in section 4.7.3.2. Acquirers are expected to enable SCA when it is required.



## Key Point

Some types of MIT transaction can be performed without using a stored payment credential.

Processing a transaction with a stored credential does not qualify a transaction as out of scope or exempt of SCA. Many CITs use stored credentials and are in scope of SCA. Each transaction must be evaluated according to its own circumstances to determine if SCA is required.

### 4.2.4 Principles for implementing SCA



Irrespective of the business processes that a merchant uses for e-commerce transactions, there are some fundamental principles that shape the approach a merchant takes to performing an authorization. These principles are summarized below and are the basis for the approach in handling each of the different scenarios in Section 5 of version 2.0 of this guide (however please also read summary guidance provided in section 5 of this version 3.0 before referring to version 2.0), and in the addendum to this guide *Implementing Strong Customer Authentication (SCA) for Travel and Hospitality*.

#### 4.2.4.1 Out of Scope transactions

Where a merchant/Acquirer is able to identify a payment transaction as out of scope of SCA, then the merchant / Acquirer must submit an authorization ensuring that appropriate information is present that allows the Issuer to recognize that the transaction is out of scope of SCA. For example, by including relevant MIT indicators, or properly flagging as MOTO. For details of the correct indicators please see Section 3.2.9.

#### 4.2.4.2 Visa principles for implementing SCA

##### 4.2.4.2.1 Implementing SCA in common payment use cases

The following Table 18 summarizes Visa's guiding principles for implementing SCA in common payment use cases for both CIT and MIT transactions.

**Table 18: Summary of common CIT and MIT payment use cases**

Transaction Type	Use Cases	Recommendation for SCA?
Cardholder Initiated	One-time purchase (with/without Credential-on-File)	Yes, but exemptions allowed
	Adjustment to existing order (e.g. change of available items or change of shipping costs)	Depending on the circumstances, SCA may not be required assuming this is addressed through T&Cs and other cardholder communications. If the update is a pricing change, SCA is required if the amount increases above the authenticated amount, but not if the amount decreases.
	Establish agreement for ongoing or one-off future payments (e.g. subscription, No Show)	SCA is required in most cases when the initial mandate is set up via a remote electronic channel <sup>60</sup>
Merchant Initiated	Executes payment (e.g. subscriptions, No Show, incremental)	Out of scope. SCA is required in most cases when the initial mandate is set up via a remote electronic channel but is not necessary for subsequent payments initiated by the merchant
	Merchant updates payment terms (e.g. change payment date, price change)	Not required assuming this is addressed through T&Cs and other cardholder communications
	Original purchase delayed or split into subsequent events with or without price changes (e.g. basket updates)	Not required as long as the original transaction was an authenticated or exempted authorization

<sup>60</sup> This does not apply in some specific cases outlined in Section 3.9 where the MIT field flags transactions which are not out of scope but where SCA has already been performed or an exemption was applied before the transaction is executed – e.g. Reauthorization (used in delayed or split authorizations) and Resubmission (resubmitted transit transactions). In Visa’s view, SCA is also required if the mandate is set up via a face to face transaction – exemptions cannot be applied.

#### 4.2.4.2.2 Implementing SCA in common non-payment scenarios

The following Table 19 summarizes Visa’s guiding principles for implementing SCA in common non-payment use cases.

**Table 19: Summary of common non-payment scenarios.**

Action	Use Cases	Recommendation for SCA Requirement
Loading of Credentials	Adding a Credential-on-File or provisioning of a token	Could be required when the cardholder is adding or provisioning a card.
	Merchant received updated payment credentials from the Issuer (e.g. Visa Account Updater, Visa Token Service)	SCA not required, but under Visa Rules must be addressed through T&Cs and other cardholder communications.
	Cardholder provides a new expiry date without any change to the card number	Not required.
	Cardholder has a payment agreement with a merchant and adds a new card number to the payment instructions	SCA is required when the initial mandate is set up via a remote electronic channel.
Card Validity Check	Check validity of PAN and expiry date using an Account Verification transaction.	Not required when used only to check validity.
Trusted Beneficiary	A merchant will send in an enrollment request to the Issuer to be added to a cardholder’s trusted beneficiaries list	SCA required on the enrollment.
Delegated Authentication	Carrying out initial cardholder verification used to enable subsequent delegated authentication	SCA required

### 4.2.4.3 Visa authentication, authorization and clearing principles for implementing SCA

Table 20 summarizes key principles that should be applied to the authentication and authorization and clearing processes.

**Table 20: Fundamental Visa authentication, authorization and clearing principles for implementing SCA**

Principle	Rationale
<b>Visa Authentication Principles</b>	
<b>1. CAVVs cannot be stored after usage.</b>	As per Visa Rules, the same CAVV can only be used for a maximum of two occasions <sup>61</sup> ; however, PCI requirements dictate that it cannot be stored post authorization. This means that a merchant can only use the same CAVV for up to two authorizations, if they are in short succession (e.g. populating two authorization requests at the same time).
<b>2. CAVVs prove that the authentication process has taken place.</b>	<p>If an Acquirer SCA exemption is being exercised, the merchant may still submit a CAVV to prove the authentication process has been performed to avoid receipt of an SCA decline code. The CAVV must always be submitted with the associated ECI value.</p> <p>Visa Rules determine that where no Acquirer SCA exemption has been applied, merchants only receive fraud liability protection for authorizations submitted with a CAVV and an ECI value 05 (indicating authentication performed) or 06 (indicating authentication was attempted but not performed).</p> <p>When an exemption has been applied, the ECI value is 07 (indicating SCA was not performed or attempted) and fraud liability protection under the Visa Rules is not applicable.</p>
<b>3. 3RI (3DS Requestor Initiated Message) must be used by merchants wishing to have fraud liability protection when more than one transaction is required to complete a single purchase.</b>	<p>Issuers will be enabling 3RI in EMV 3DS 2.1 and it will be an integral feature within EMV 3DS 2.2. This enables merchants to obtain authentication data (CAVV, ECI) in the absence of the cardholder for transactions previously authenticated<sup>61</sup>.</p> <p>The feature can be used to enable merchants to effectively manage some payment use cases by for example:</p> <ul style="list-style-type: none"> <li>• Allowing an authorized entity in a Multi-Party Commerce scenario occurring in the Travel &amp; Entertainment industry to request a CAVV on behalf of a merchant.</li> <li>• Allowing merchant to obtain a new CAVV in case of split or delayed shipment when one or more item is not ready for shipment until a later date.</li> </ul>

<sup>61</sup> Visa has temporarily amended this rule to allow the reuse of the CAVV up to five times, until 1 September 2022, for split shipment scenarios and scenarios where transactions are associated with bookings via travel agencies. The previous rule expired on 1 September 2020 and Visa has now extended the expiration date to 1 September 2022. For more information please see VBN Article ID: AI10292 *Update to CAVV—Exceptions to Reuse in Europe 20 August 2020*.

Principle	Rationale
	<ul style="list-style-type: none"> <li>Requesting a new CAVV to maintain liability protection when authorization is sought more than 90 days after a transaction has been authenticated.</li> </ul> <p>The merchant needs to send prior authentication information and original ACS Transaction ID when submitting a 3RI transaction.</p> <p>A CAVV obtained under 3RI should be processed under the same rules as a CAVV obtained when the card holder was presented (e.g. cannot be stored after use, valid for fraud liability protection up to 90 days, etc.).</p>
<b>4. Token Authentication Verification Value based on Cloud Token Framework (CTF TAVV) can be used by qualifying token requestors for cardholder authentication</b>	In some cases, qualifying token requestors can use the CTF TAVV as evidence of cardholder authentication. In such cases a CAVV is not required for SCA compliance. CTF TAVVs used in this way do not qualify the merchant for liability protection under the Visa Rules. More information is provided in the 'Changes to the Visa Token Service to Support Cloud Token Framework' articles in the October 2019, April 2020 and October 2020 Business Enhancements releases.
<b>5. Token Transactions require a TAVV unless they are being submitted as MITs</b>	Visa requires a TAVV (existing or new CTF TAVV) to be present in all Token transactions unless the transaction is identified as a Merchant Initiated Transaction.
<b>Visa Authorization Principles</b>	
<b>6. SCA requirements apply to Tokens and PANs</b>	Visa Tokens can be used in the place of PANs throughout the payments eco-system. Therefore, any merchant or Acquirer using Visa Tokens for financial transactions should use the same criteria for their SCA decisions as they use for PANs.
<b>7. An MIT can only occur after an initial CIT has been performed to establish a customer agreement</b>	<p>SCA is not required for an MIT so long as the initial mandate (CIT) is set up via a remote channel by applying SCA.<sup>62</sup></p> <p>In Visa's view SCA is not required for the CIT in the following cases when an exemption can be applied:</p> <ul style="list-style-type: none"> <li>The CIT is split or delayed</li> <li>The CIT is resubmitted in the case of contactless transit transactions</li> <li>The CIT qualifies for the secure corporate payments exemption</li> </ul> <p>In Visa's view, SCA is also not required when the mandate is set up via MOTO.</p>

<sup>62</sup> Note: In Visa's view, SCA is also required if the mandate is set up via a face to face transaction – exemptions cannot be applied.

Principle	Rationale
<p><b>8. MITs must be properly indicated as MITs to ensure they are treated as out of scope of SCA</b></p>	<p>If a merchant initiates an MIT, the transaction is out of scope of SCA and Issuers must be able to recognize it as an MIT. In the Visa system, this is done by the merchant/Acquirer adding the MIT indicators to any MIT.</p> <p>When receiving transactions that are properly indicated as MITs using the MIT Framework, Visa will automatically populate the value of "1" in Field 34 (Tag 80, Dataset ID 02). This enables Issuers to recognize a transaction as an MIT (and therefore out of scope of SCA) by simply checking for the value of "1" in that tag. Issuers can also recognize transaction as MITs using the indicators from the Visa MIT Framework.</p>
<p><b>9. Merchants need to store the Transaction ID of the CIT (or of a previous MIT for 3 of the MIT types as defined in section 3.9.2.1) that established the agreement for future MITs.</b></p>	<p>An MIT must reference the transaction during which the MIT was set up by either including the Transaction ID of the original CIT (or the Transaction ID of a previous MIT - applicable only to certain types of MIT) in the authorization message. Therefore, merchants who might perform MITs need to store the Transaction ID of their associated CIT (or a previous MIT) until no further MITs are required and any agreement with the customer is complete.</p>
<p><b>10. Merchants should only request authorization when the goods are available and ready to be shipped</b></p>	<p>A merchant must not clear a transaction before goods have been shipped (as per Visa Rule # 27797). In addition, merchants should only request authorization when they have confirmed that the goods are available and ready to be shipped. This minimizes the impact to the customer's open to buy and ensures that the CAVV is not used ineffectually.</p>
<p><b>11. Authorizations are valid for a maximum of up to 7 days</b></p>	<p>If an authorization cannot be fully cleared after 7 calendar days<sup>63</sup> have elapsed, the merchant must submit a reversal for the un-cleared amount. If the transaction can subsequently be fulfilled, the merchant must first perform a re-authorization (or several if shipment is split). In the PSD2 context, these re-authorizations must be performed with MIT re-authorization indicators to ensure authentication does not need to be performed again unnecessarily.</p>
<p><b>12. Merchants must perform an additional account verification and address CAVV expiry if a transaction is delayed by more than 90 days</b></p>	<p>Merchants should avoid being in the position of delaying authorization for more than 90 days.</p> <p>If a merchant cannot avoid being in a position of a greater than 90-day delay, it needs to obtain a new transaction ID for usage in a delayed authorization to ensure that the transaction meets Visa processing requirements, as if the transaction was done with a token, it will no longer be valid. As such, the merchant should perform a new account</p>

<sup>63</sup> Different authorization validity periods may apply to some merchants and transaction types, particularly in the T & E sector. For example, mass transit transaction approvals are only valid for 3 calendar days. Refer to Visa rule ID #0029524 for more information.

Principle	Rationale
	<p>verification and the Transaction ID of this account verification must be stored for use in the delayed authorization. If a token is used, this new account verification will require a new TAVV.</p> <p>In addition, as per Visa Rules, the CAVV offers fraud liability protection for only the first 90 days after its creation. If needed, it can still be used past 90 days, albeit, without fraud liability protection. For delays over 90 days:</p> <ul style="list-style-type: none"> <li>• A merchant wishing to receive fraud liability protection must first use 3RI (if available) to obtain a new CAVV (with ECI 05) for the relevant amount to include in the authorization.</li> <li>• If 3RI is not available or the merchant wishes to proceed without fraud liability protection, the merchant may submit a CAVV (and its associated value of 05) that is older than 90 days, but Issuers will still have dispute rights. The benefit for the merchant is that including a valid CAVV should prevent the Issuer declining with an SCA decline code <sup>64</sup>.</li> </ul> <p>If the original CAVV was obtained using an Acquirer exemption (i.e. has an associated value of 07) – there is no need to use 3RI to obtain a new CAVV, as fraud liability protection does not apply.</p>
<p><b>13. When an authorization must be delayed until after the cardholder is no longer available, the merchant must always:</b></p> <ol style="list-style-type: none"> <li><b>perform an account verification and any required authentication at checkout</b></li> <li><b>indicate the delayed authorization with appropriate indicators, such that the Issuer knows that the cardholder is not available for authentication</b></li> </ol>	<p>If an authorization cannot be performed at checkout and must be delayed, the merchant must perform an account verification immediately (following any required authentication) and store the Transaction ID of this account verification transaction. Later, when the shipment is ready to be made, the merchant must submit a delayed authorization with message reason code (MRC) 3903 and the transaction ID of the account verification (original CIT). In such case, although a CAVV is not required as the transaction is indicated as an MIT, a delayed authorization can still optionally include a CAVV for the sole purpose of qualifying the merchant for fraud liability protection. If authentication was performed via 3-D Secure and a CAVV was obtained, the merchant process differs depending on whether the CAVV was included in the original CIT or not.</p> <p><b>CAVV used in original CIT:</b> If the CAVV was submitted during the account verification (original CIT), then the delayed authorization can either be submitted with a new CAVV and associated ECI value (using 3RI, if available<sup>65</sup>), with the original CAVV (as an interim, if 3RI is not yet available, up to a maximum of five times – note that liability protection is in this</p>

<sup>64</sup> A merchant should not submit a CAVV older than one year as the CAVV will fail validation.

<sup>65</sup> For more information please see VBN Article ID: AI10292 *Update to CAVV—Exceptions to Reuse in Europe* 20 August 2020. Note: This interim arrangement can only be applied until 01 Sept 2022.

Principle	Rationale
	<p>case limited to the 90 days validity of the CAVV)<sup>65</sup> or without a CAVV (in which case, without fraud liability protection).</p> <p><b>CAVV not used in original CIT:</b> If the CAVV was not submitted during account verification (original CIT), then the CAVV must be stored for later submission in the delayed authorization. If multiple delayed authorizations are required to complete the purchase (e.g. due to split shipments), then the merchant and Issuer must be aware that each subsequent delayed authorization must have its own separate CAVV (e.g. using 3RI) for fraud liability protection, since the original CIT does not contain a CAVV that can be referenced. If 3RI is not yet available, the CAVV may be submitted as an interim approach up to a maximum of five times, but note that liability protection is in this case limited to the 90- days validity of the CAVV)<sup>65</sup>.</p> <p><b>Important note:</b> This principle ensures a consistent approach in handling payment scenarios with delayed authorization that works for both PAN and Token<sup>66</sup>.</p>
<p><b>14. Transaction amounts can vary between authentication, authorization and clearing - the amount authorized and cleared can be lower than the authenticated amount but not higher</b></p>	<p>Dynamic Linking requires that the transaction amount and the identity of the payee at authentication must be included in the authentication code (CAVV). The EBA has stated that the final amount cannot increase above the authenticated amount without further authentication.</p> <p>The same does not apply where the final, authorized amount is lower than the authenticated amount. In these cases, no re-authentication is required.</p> <p>As a result, Visa eliminated the existing authorization tolerance limits that allow e-commerce and tipping merchants to clear an amount greater than the authorized amount for EEA acquired merchants (currently still allowed for UK acquired merchants).</p> <p>For guidance on options for dealing with variations in amount please see section 4.2.2</p>
<p><b>15. Issuers must not respond to the authorization request for out of scope transactions with an SCA decline code (1A)</b></p>	<p>An Issuer must not use an SCA decline code for transactions deemed out of scope from a regulatory perspective or ask for authentication in response to authorization requests for transactions legitimately identified as out of scope (MITs, MOTO One-Leg-Out or transactions performed with an anonymous payment instrument). In the case of MITs, the</p>

<sup>66</sup> If the Merchant / Acquirer knows with absolute certainty that the payment credential is a PAN, then they could implement an alternative approach, whereby they do not need to submit an account verification immediately, but rather retain the CAVV to include it in a standard authorization when the goods are ready to be shipped (i.e. without MRC 3903 or an initial Transaction ID).



Principle	Rationale
	<p>cardholder is not available for authentication, therefore it is essential that merchants use the MIT framework to enable Issuers to identify MITs where the cardholder is not available.</p>
<p><b>16. Grandfathering can be applied to MITs performed based on agreements made prior to the regulatory enforcement date</b></p>	<p>A merchant with an existing agreement with a customer established prior to the regulatory enforcement date does not need to establish a new agreement with their customer with SCA. Instead, all MIT authorizations performed after the enforcement date can reference either the “initial” CIT, or the transaction ID of any previous related transaction processed before the enforcement date (CIT or MIT). The transaction ID of the selected transaction must be stored and always included in future related MITs as evidence of an existing agreement with the customer. The selected transaction does not need to meet SCA requirements (e.g. it does not need to have had a CAVV) given that it was performed prior to the enforcement date.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• In an established <b>subscription</b>, the transaction ID of any previous MIT of the series can be used.</li> </ul> <p>For transactions described under the MIT framework as Industry Specific Business Practices, the transaction ID of the previous CIT can be used, even if it wasn’t authenticated, provided it was performed prior to the enforcement date.</p>
<p><b>17. When setting up an agreement to process future MITs, only authenticate and authorize for amount needed on the day of the agreement</b></p>	<p>When setting up an agreement that also includes an initial charge (e.g. a magazine subscription), the merchant should only authenticate and authorize for the amount due immediately. For example:</p> <ul style="list-style-type: none"> <li>• For subscriptions (recurring and unscheduled credential on file (UCOF) transactions in the Visa system): <ul style="list-style-type: none"> <li>• If the first monthly payment is 5 Euros, authenticate and authorize for 5 Euros</li> <li>• If a free trial period applies, authenticate and authorize for zero amount</li> <li>• If the first payment is a reduced promotion amount of 2 Euros, rising to 5 Euros after 3 months, authenticate and authorize for 2 Euros.</li> </ul> </li> <li>• For installment/prepayments: <ul style="list-style-type: none"> <li>• If the first installment/deposit is not due at the time of the agreement, authenticate and authorize for zero amount,</li> <li>• If the first installment/deposit is due at the time of the agreement, authenticate and authorize for that amount.</li> <li>• No amount should be authenticated or authorized in the case where an agreement includes an allowance for conditional future charges using</li> </ul> </li> </ul>

Principle	Rationale
	<p>other Industry Specific MITs such as “No Show”, Incremental or Delayed Charges. For example, if booking a hotel with no deposit required, but with payment due in full in case of No Show, authenticate and authorize for zero value at the time of booking.</p> <p>Reauthorizations MITs for open orders and aggregated payments are an exception to this principle, where it is possible for the merchant to authenticate the transaction for a maximum estimated amount that the basket order can have.</p>
<b>Visa Clearing Principles</b>	
<b>18. Multiple clearing records can be submitted for a single authorization</b>	<p>This principle can be applied when an order cannot be fulfilled in a single shipment. It is Visa’s recommended best practice to handle multiple shipments via multiple clearing records rather than via multiple authorizations. Because a CAVV is not included in clearing, submitting multiple clearing records to fulfil a single authorization does not impact merchant fraud liability.</p>

#### 4.2.5 Who can apply exemptions?



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

**Table 21: Summary of who may apply an exemption<sup>67</sup>**

Exemption	Issuer	Acquirer
Trusted beneficiaries	Yes	No <sup>i</sup>
Transaction Risk Analysis (TRA)	Yes	Yes <sup>ii</sup>
Low Value Transactions	Yes	Yes <sup>ii, iii</sup>
Secure corporate payment processes & protocols	Yes <sup>iv</sup>	N/A <sup>v</sup>

<sup>67</sup> Adapted from Table 2 in the EBA Opinion Paper on the Implementation of the RTS on SCA and CSC 13 June 2018.

## Notes:

- i. Under the PSD2 regulation, an Acquirer may not apply the trusted beneficiaries exemption, however 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 the 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.
- ii. 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.
- iii. While the regulation allows for the Acquirer to apply the exemption, this is not practically feasible as the Acquirer does not have visibility of the velocity limits that apply to the exemption.
- iv. Issuers who have demonstrated to NCAs that applicable processes and protocols meet the requirements of the regulation should apply the exemption when a transaction is received with the secure corporate exemption indicator.
- v. Merchants who process transactions originating from within secure corporate environments, may be able to flag to their Acquirer, who flags to the Issuer using the secure corporate exemption indicator, that they consider the transaction qualifies for the secure corporate payments exemption. Secure corporate environments could for example, and subject to the view of local regulators, include corporate purchasing or travel management systems.

Note that Visa does not provide any indicator for the recurring transactions exemption as the exemption is not used in the Visa system; Visa transactions that would use the recurring payments exemption are MITs and as such are out of scope of the SCA requirements entirely. Visa provides a way to flag recurring payments as MITs.

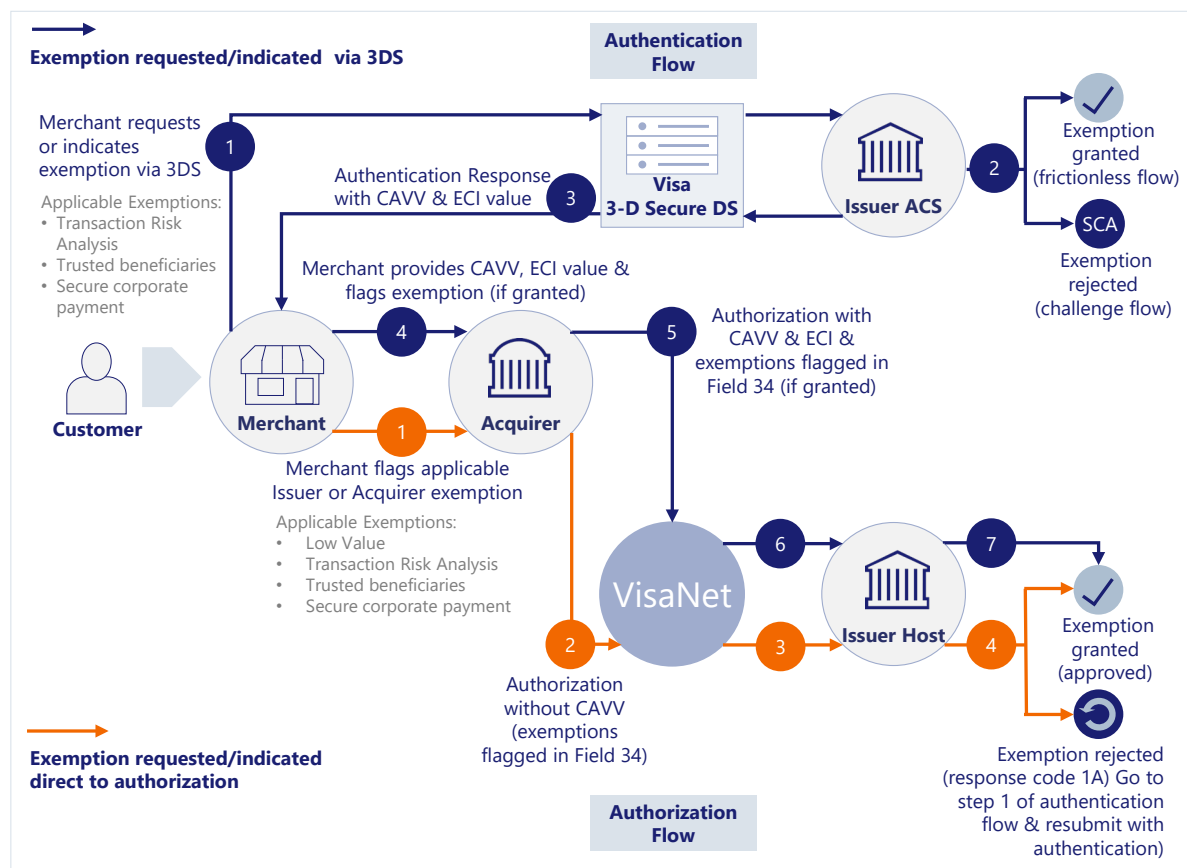
### 4.2.6 Options for merchants & Acquirers regarding exemption application



If a payment transaction is in scope of PSD2 (and SCA), then the merchant / Acquirer must determine whether an SCA exemption can be exercised or not.

A merchant / Acquirer can exercise an exemption via the EMV 3DS 2.2 authentication flow, or directly via a VisaNet Authorization, as shown in Figure 16 below:

**Figure 16: Visa model to execute SCA exemptions**



- Exemption via 3DS authentication:** The merchant can exercise an exemption via a EMV 3DS message first, before performing an authorization request. This is done by setting the relevant indicators in the EMV 3DS message and in the subsequent authorization. The advantage of this approach is that if the exemption is rejected by the Issuer, the cardholder is still present to complete any required SCA challenge, even if authorization will be delayed. Merchants should be aware that if taking this approach, the exemption exercised during authentication, so long as it is accepted by the Issuer, must be re-stated in the authorization message along with the CAVV and ECI value received at the authentication step.
- Exemption direct to authorization:** The merchant can go directly to authorization, flagging the exemption used in Field 34. The advantage of this approach is that the authentication step can be skipped altogether, if the Issuer accepts the exemption. Furthermore, the low value exemption can only be indicated by an Acquirer in the authorization flow as there is no 3DS indicator. However, merchants considering this option should be aware that the Issuer can decline the exemption and request SCA. In the case where authorization is delayed and the Issuer rejects the exemption, the cardholder will no longer be available to perform authentication. Acquirers/merchant should review market specific requirements before adopting this exemption option, since some markets may require exemptions to be raised via an authentication message first. For additional guidance, please refer to section 4.3.4.
- No exemption exercised:** The merchant can perform authentication and authorization without populating any exemption indicators in 3DS and in authorization Field 34.

## 4.3 Step by step guide to SCA optimisation



### 4.3.1 Individual transaction decision flows

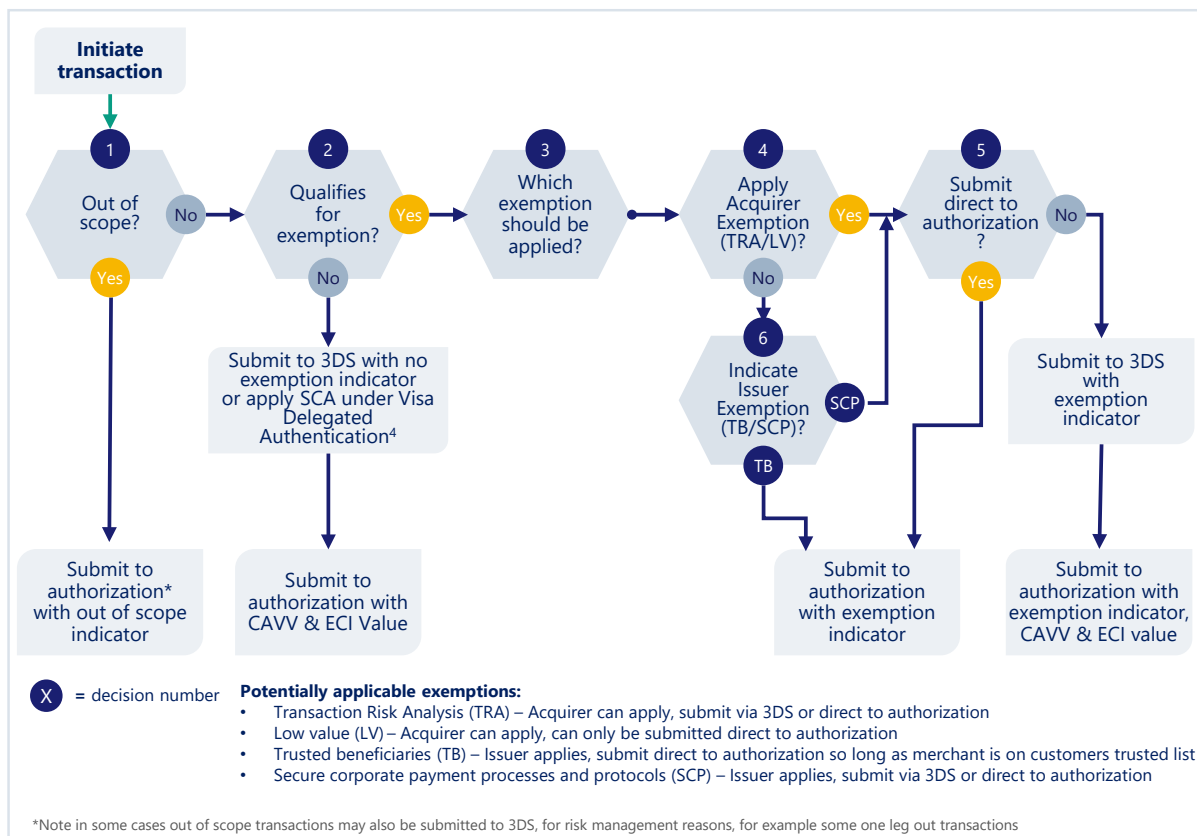


At the individual transaction level, merchants, Acquirers and Issuers move through a sequence of decision points to determine whether:

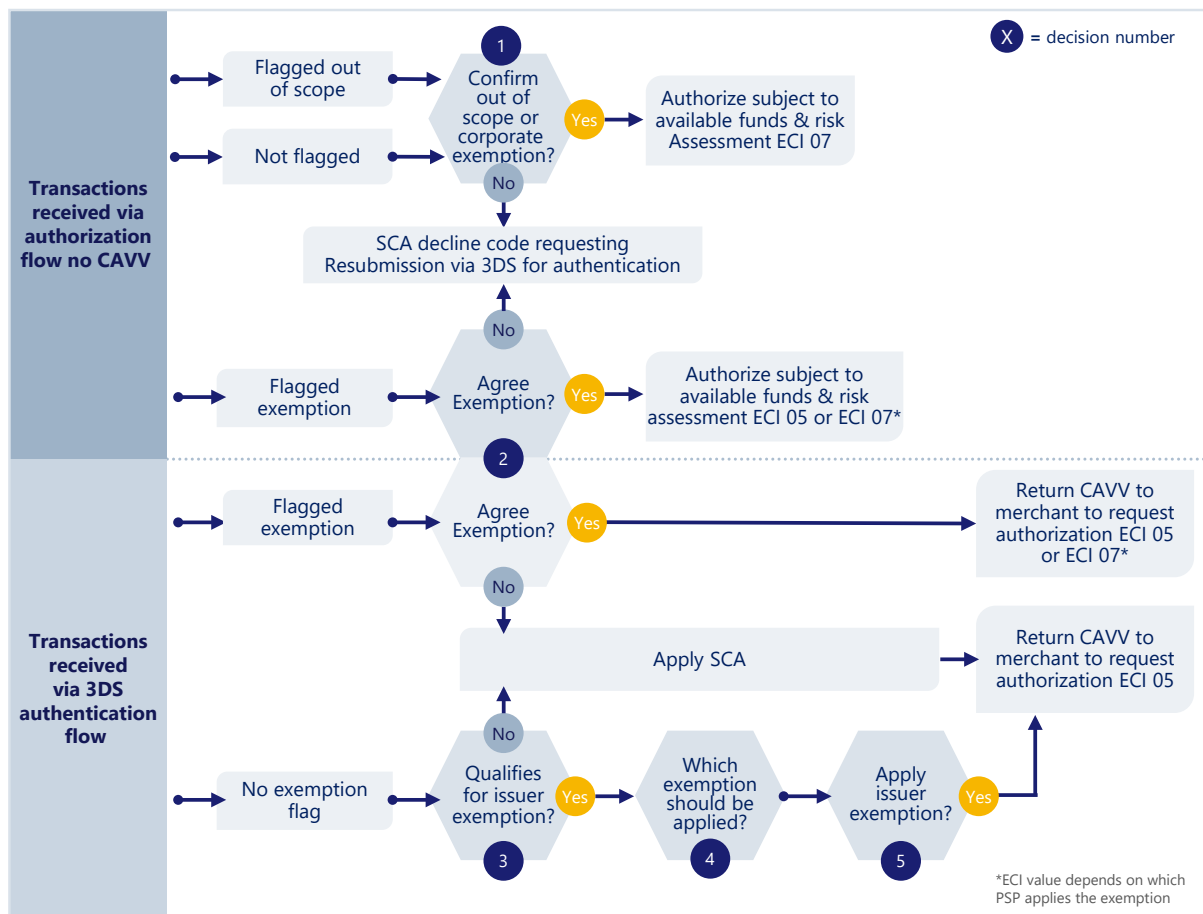
- The transaction is in or out of scope of PSD2 SCA
- The transaction qualifies for an exemption
- Which qualifying exemption should be applied
- In the case of merchants/Acquirers, how the transaction should be routed, via 3DS or direct to authorization

These decision points are summarized in Figures 17 and 18 below:

**Figure 17: Key merchant/Acquirer decision points**



**Figure 18: Key Issuer decision points**



An overview of the considerations to take into account at each of these decision points is included in the following sections. A detailed summary of each decision point is given in Appendix A.5.

### 4.3.2 Key steps to minimising friction



There are a number of policy steps that merchants, Acquirers and Issuers can take to minimise any friction experienced by customers making remote electronic payments, while maintaining compliance with the PSD2 SCA regulation. Reducing customer friction is essential to optimising customer experience and minimising transaction abandonment.

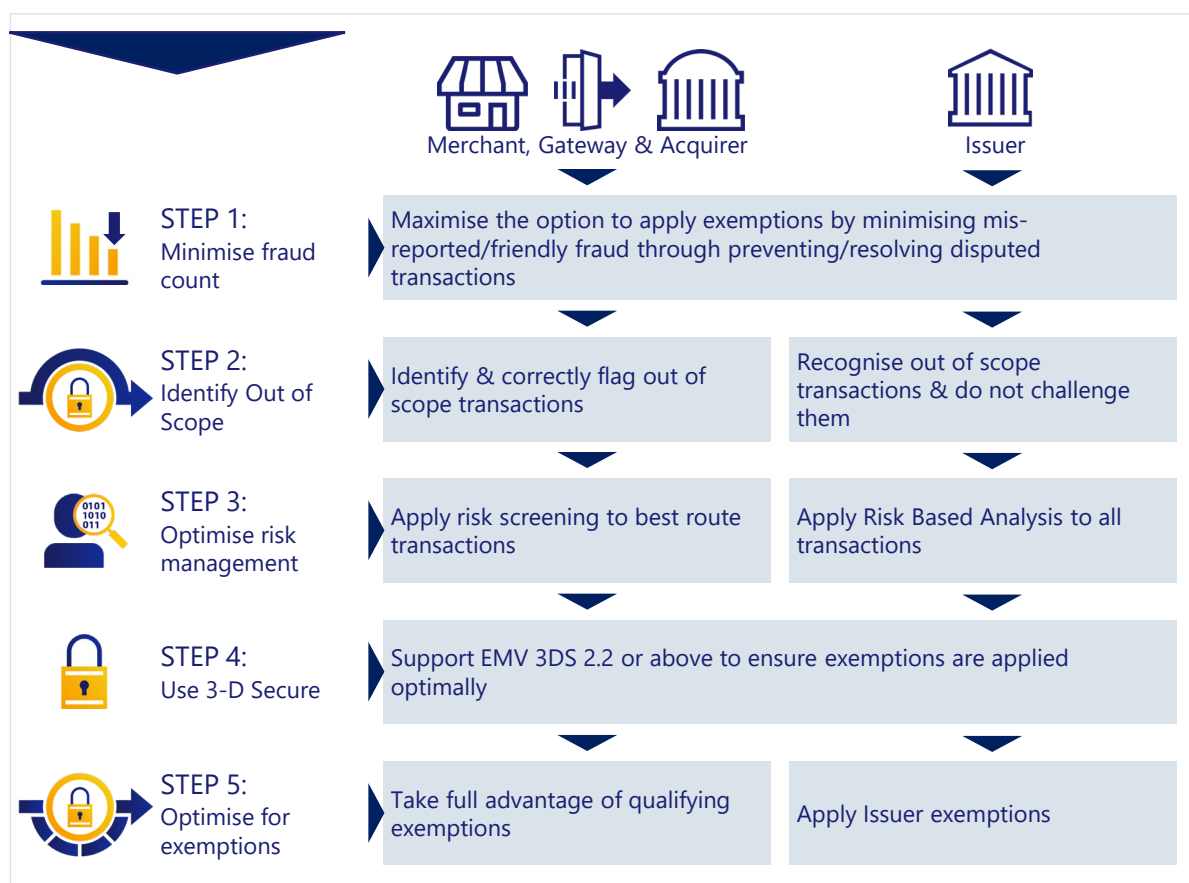
The steps that merchants, Acquirers and Issuers should take to minimise friction can be grouped into two clear stages:

- Stage 1: Minimising the need for SCA challenges
- Stage 2: Creating a challenge process offering minimal friction when SCA challenges are required

This section provides merchants, Acquirers and Issuers with guidance on Stage 1. See section 4.6 for guidance on Stage 2.

The key policy steps required to minimize the need for SCA challenges are summarised in Figure 19 below and the following sections. For more detail, please refer to the *PSD2 SCA Optimisation Best Practice Guide*:

**Figure 19 Stage 1: Minimising the need for SCA challenges**



### 4.3.3 Summary of the Steps

#### 4.3.3.1 Step 1: Minimise fraud count



Disputes are often marked as fraud even when they are raised only because customers have trouble recognizing transactions and not because the transaction was unauthorised. Visa analysis indicates that fraud is reported 90% of the time a dispute is submitted<sup>68</sup>.

Such disputes can artificially and unnecessarily inflate fraud counts, limiting the ability of Acquirers and Issuers to apply the TRA exemption and potentially limiting the ability of individual merchants to be considered for the application of certain exemptions<sup>69</sup>.

Visa’s experience has shown that a significant proportion of both disputes and transactions unnecessarily categorised as fraudulent can be avoided if customers and Issuers can be provided with additional information, such as the item purchased, to help customers validate transactions before they formally ask for a transaction to be disputed.

If merchants provide this information to Issuers it enables them to deal more effectively with customer queries, improving customer satisfaction and removing these transactions from the

<sup>68</sup> Source: Visa analysis from Visa Resolve Online statistics.

<sup>69</sup> Acquirers are more likely to consider applying exemptions to transactions from low fraud rate merchants. In some specific cases, for example, the Visa Trusted Listing program which facilitates the application of the trusted beneficiaries exemption, merchants need to meet fraud rate targets to be enrolled and remain within the program.

fraud count. This can potentially improve the risk score of every transaction a merchant processes, while increasing the ability of Acquirers and Issuers to apply the TRA exemption. Merchants can also benefit by reducing revenue losses from disputes, as well as increasing their ability to qualify for the application of key exemptions.

Verifi, a Visa company, offers a suite of related Pre-dispute Products to help both merchants and Issuers avoid and resolve such disputes. For more information see section 3.8.2.

#### 4.3.3.2 Step 2: Identify and flag out of scope transactions

Merchants who process out of scope transactions need to ensure that they can identify these transactions and populate the appropriate authorization indicators, as defined by their Acquirer. Note it is important that merchants check how their payment gateway/Acquirer would like them to identify MITs and other out of out of scope transactions. Some payment gateways/Acquirers use a proprietary standard for merchant flags and then convert the flags to the appropriate card scheme standard before submitting an authorization request.

Issuers must be able to recognise every type of out of scope transaction and must not decline or request authentication for transactions that have been flagged as out of scope by the Acquirer<sup>70</sup>.

For more information on identifying out of scope transactions and other transactions that do not require SCA please refer to section 3.2.9.

#### 4.3.3.3 Step 3: Optimise risk management

Visa recommends that merchants undertake risk screening on transactions before submitting them to authentication or authorization. Issuers are required to apply Risk Based Analysis (RBA) to all transactions and will always take the final decision on whether to allow an exemption to be applied to a particular transaction when it is indicated by the merchant or Acquirer.

At its simplest level, RBA is based upon rules set by or in conjunction with the merchant to assess the risk of a transaction based upon simple characteristics of the transaction. More sophisticated solutions increasingly use machine learning based risk models and multiple datapoints to provide a much more accurate assessment of risk and minimise both fraud and false positives.

The approach taken by merchants will depend upon their size, resources and the risk profile of their business.

- Smaller merchants may choose by default to submit all of their transactions via 3DS leaving the Issuer to risk assess them and decide which transactions qualify for exemptions. However, a merchant who applies no RBA or fraud screening risks a higher fraud rate, the application of fewer exemptions and higher customer friction. It is recommended that such merchants speak to their payment gateway, Acquirer or 3DS server provider to check what risk analysis and screening services they are able to offer.
- Larger and enterprise merchants should look to adopt more proactive strategies using more sophisticated risk tools to minimise fraud rates and take advantage of

---

<sup>70</sup> For more information please refer to Section 4.5 of *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area Visa Supplemental Requirements*.



the ability to apply the Acquirer exemption and send transactions direct to authorization, to minimise the impact on customer experience and reduce authentication costs.

Merchants must align with their gateway/Acquirer to ensure that their SCA exemption strategy is supported.

Managing risk effectively will enable Issuers to maximise their ability to apply exemptions. Issuers should aim to implement risk strategies that balance the need to keep fraud low whilst at the same time avoiding the need to challenge every single transaction. In the case of the TRA exemption, keeping fraud rates within the reference fraud rate for the highest achievable transaction value band can be achieved by making full use of 3DS data. For more information on Issuer application of RBA please refer to section 3.3.9.

#### 4.3.3.4 Step 4: Use 3D Secure

3-D Secure (3DS) is the leading industry standard solution being used across the card payments industry to apply SCA.

The latest version of 3DS, EMV 3DS 2.2, provides critical new functionality that is fundamental to the optimisation of the application of PSD2 SCA and all permitted exemptions. All Issuers are mandated to support EMV 3DS 2.2 since September 14, 2020 and Acquirers are mandated to ensure their merchants are connected to vendors who support it since 16 October 2020.

Merchants must support 3DS to facilitate the application of SCA which is required under PSD2 and Visa strongly encourages merchants and Acquirers to support EMV 3DS 2.2 as early as possible.

For more information on 3DS refer to section 3.3.

#### 4.3.3.5 Step 5: Optimise use of exemptions

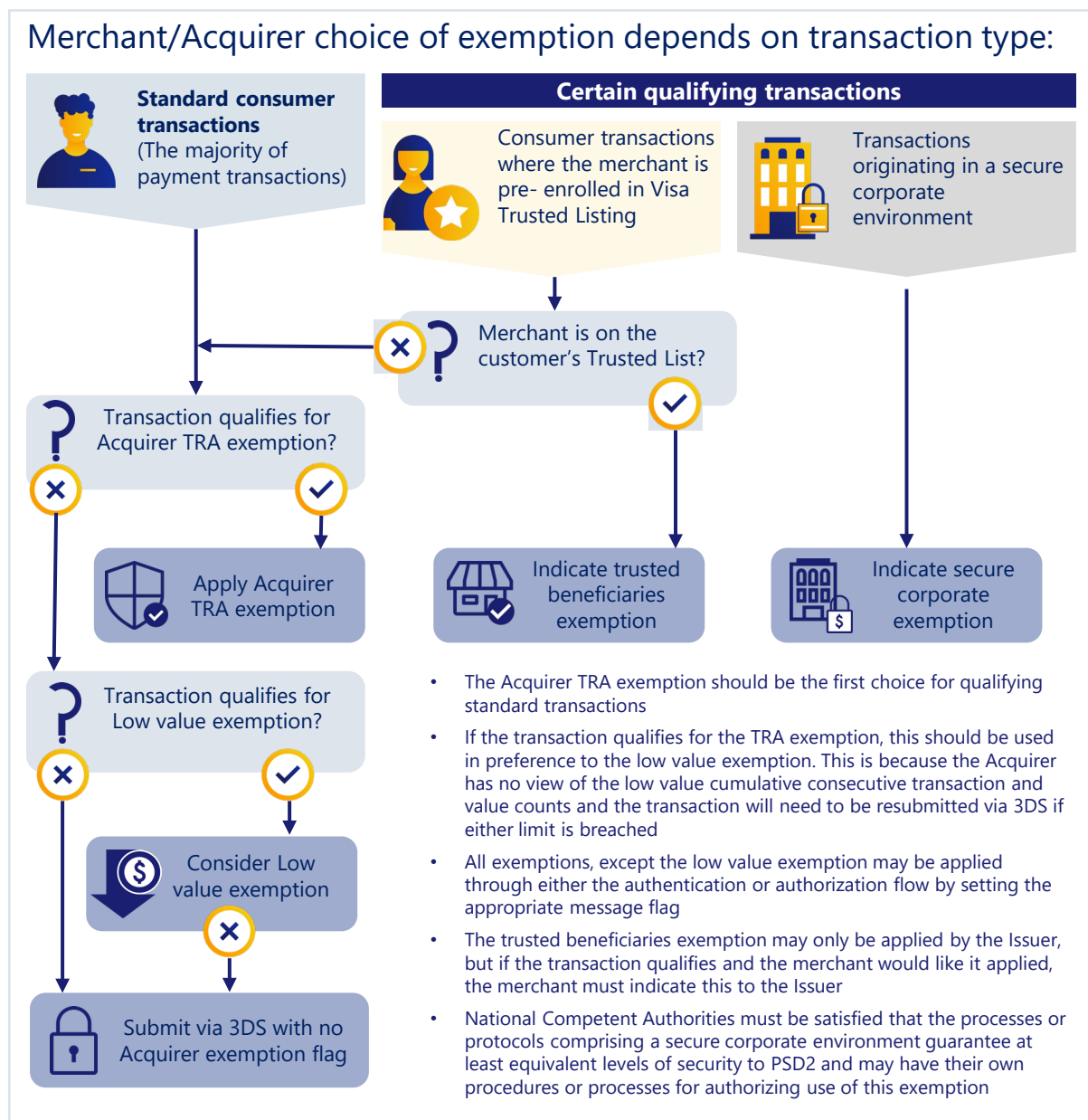
The logic shown in Figure 20 should help merchants and Acquirers to select which, if any, allowable exemption to apply or request.

Issuers may apply any of the exemptions.

Acquirers may, subject to transaction value and their fraud rate, apply either the TRA exemption or the low value transaction exemption. The EBA have confirmed that Issuers and Acquirers must take into account fraud on all transactions subject to SCA in the calculation of their fraud rate, regardless of which PSP took liability, for example by applying the TRA exemption. This may lead to Issuers being less likely to accept Acquirer TRA indicators as any fraud on these transactions will impact the Issuer's fraud rate. Fraud on transactions where the Issuer has applied a TRA exemption will also impact the Acquirer's fraud rate. This reinforces the benefit for merchants to undertake risk screening of transactions before submitting them for authorization.

Merchants may 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. The order in which exemptions should be applied or requested by merchants and Acquirers depends upon the transaction type and whether the transaction qualifies.

**Figure 20 Prioritisation of exemptions: merchant/Acquirer**



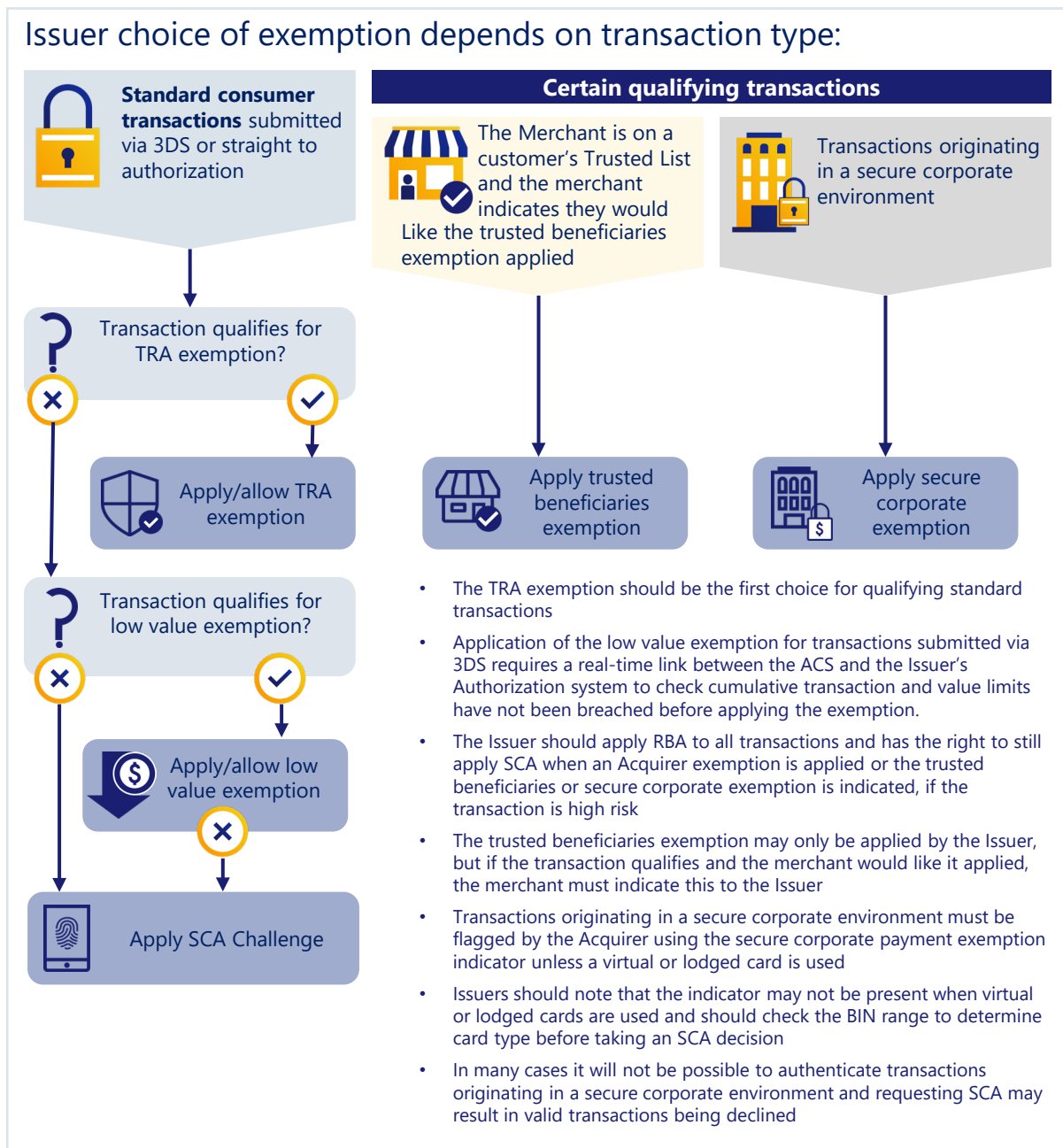
Merchants should note that only one exemption should be applied or indicated in a given transaction and that Issuers have the final say on whether an exemption can be applied and may choose to apply a challenge to a transaction flagged with an exemption indicator if they consider it to be high risk.

Issuers should apply risk analysis to all transactions and generally:

- When transactions are submitted by Acquirers with an exemption indicator (via 3DS or direct to authorization), allow the exemption unless analysis indicates the risk is high
- When transactions are submitted by Acquirers via 3DS without an exemption indicator, apply exemptions to all transactions that qualify

The most appropriate exemption will depend upon the transaction type and the qualifying criteria, as shown in Figure21:

**Figure 21: Prioritisation of exemptions: Issuer**



More information on the application of individual exemptions is included in Section 4.5 below.

Merchants and Acquirers should also be aware that:

- Issuers may have less data on which to assess transactions sent directly to authorization than they would have for transactions submitted via EMV 3DS and they may therefore be more likely to request resubmission via EMV 3DS.
- The issuing of an SCA decline code and resubmission via EMV 3DS is likely to add latency to the processing of a transaction.
- If there is a delay between the cardholder initiating the transaction and authorization being requested and the Issuer requires resubmission via 3DS, the cardholder may no longer be available to complete authentication resulting in a decline.

Merchants and Acquirers should therefore exercise caution when submitting transactions straight to authorization.

Acquirers must include an exemption indicator in the authorization request if they are submitting transactions under an Acquirer exemption or asking the Issuer to consider applying an Issuer exemption. Transactions without exemption indicators or without having had SCA applied, after the regulatory enforcement date<sup>71</sup> are likely to receive an SCA decline code from the Issuer.

Acquirers should have policies in place on the risk profile of transactions that may be sent straight to authorization with exemption indicators set in order to provide merchants that qualify with the opportunity to take advantage of the facility while minimizing the risk of fraud and SCA decline code.

Merchants should consult their Acquirers to help determine under what circumstances it may be appropriate to submit transactions straight to authorization with an exemption indicator, in line with Acquirer policies.

### Key Point

Acquirers must also ensure they pass any SCA decline code (1A) on to their merchants rather than aggregating them with other decline codes such as "Do Not Honour" so merchants have visibility of the nature of the decline and are able to respond to this particular message to re-submit the transaction.

#### 4.3.4 Guidance to Issuers on assessing transactions submitted direct to authorization



Issuers should have policies in place on risk assessing transactions that are sent straight to authorization with or without exemption indicators set. These should aim to minimize the unnecessary application of an SCA decline code while staying in line with the Issuers risk management policy and the requirement to decline or "soft decline" (by using an SCA decline code) transactions that are in scope of SCA but are submitted to authorization without SCA or without an exemption indicator after the regulatory enforcement date. See section 3.2.3.3 for information on the use of the SCA decline code for cross border transactions including transactions between the EEA and the UK during the period between the respective enforcement dates for the EEA and the UK.

In some markets, national managed implementation plans have been agreed between financial services and retailer associations and NCAs. Some of these plans include a progressive introduction of "soft declines" ahead of the enforcement date. Issuers should check and comply with these plans as appropriate.

---

<sup>71</sup> After the regulatory enforcement date, Issuers should be expected to decline transactions that are in scope of SCA submitted without SCA and without a correct indicator. In some markets the Issuers will start progressively introducing these so called "soft declines" ahead of the enforcement date under national managed implementation plans agreed between financial services and retailer associations and NCAs. Merchants and Acquirers should check the status of such plans in their local markets.

#### 4.4 Liability for fraud-related chargeback



Tables 22, 23 and 24 below summarize how liabilities for fraud-related chargeback apply between the Issuer and the Acquirer under the Visa Rules for the application of exemptions, application of Delegated Authentication and resilience and for out of scope transactions. Exemptions applied or indicated by the Acquirer must have an exemption indicator in F34 in the authorization request to be considered valid by the Issuer.

Transactions for which SCA is applied are at Issuer liability ECI 05.

Please note that that disputes liability under the Visa Rules may differ from “regulatory liability” under PSD2. For example, the payee’s PSP cannot apply the trusted beneficiaries exemption, therefore, the Issuer is deemed to apply the exemption and is liable for fraud under PSD2 if an authorization was approved without appropriate authentication under the Visa Trusted Listing Program. However, 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 protection from fraud-related chargeback liability under the Visa Rules, 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.

**Table 22: Summary of EMV 3DS indicators and Field 34 indicators for exemptions and associated Fraud Liability**

Exemption	Acquirer or Issuer applied	Authentication		Authorization	Fraud liability under Visa Rules <sup>72</sup>
		Merchant populated Exemption indicator in EMV 3DS Yes or No	ECI Value	Acquirer populated exemption indicator in authorization F34 Yes or No	
Transaction Risk Analysis <sup>73</sup>	Submitted for authentication via 3DS prior to authorization				
	Acquirer	Yes	7	Yes	Acquirer
	Issuer	No	5	No	Issuer
	Submitted straight to authorization				
	Acquirer	N/A	7	Yes	Acquirer
	Issuer	N/A	7	No <sup>74</sup>	Acquirer

<sup>72</sup> Regulatory liability may differ.

<sup>73</sup> The TRA exemption indicator is only available in EMV 3DS version 2.2 or higher (not in EMV 3DS 2.1).

<sup>74</sup> It is not recommended (yet allowed) for an Acquirer to submit this type of transaction without a value in Field 34. It is best practice for the Acquirer to populate an exemption indicator or other informational indicator (Visa Delegated Authentication, Resilience indicator or Deferred authorization Indicator) in F34 when no authentication data is sent to the Issuer in an authorization request.

Exemption	Acquirer or Issuer applied	Authentication		Authorization	Fraud liability under Visa Rules <sup>72</sup>
		Merchant populated Exemption indicator in EMV 3DS Yes or No	ECI Value	Acquirer populated exemption indicator in authorization F34 Yes or No	
Low Value	Submitted for authentication via 3DS prior to authorization				
	Issuer <sup>75</sup>	N/A	5	No	Issuer
	Submitted straight to authorization				
	Acquirer	N/A	7	Yes	Acquirer
	Issuer	N/A	7	No <sup>74</sup>	Acquirer
Secure Corporate Payment <sup>76</sup>	Submitted for authentication via 3DS prior to authorization				
	Issuer	Yes	7	Yes	Acquirer
	Issuer	No	5	No	Issuer
	Submitted straight to authorization				
	Issuer	N/A	7	Yes	Acquirer
	Issuer	N/A	7	No <sup>74</sup>	Acquirer
Trusted Beneficiaries <sup>77</sup>	Submitted for authentication via 3DS prior to authorization				
	Issuer	Yes	5	Yes	Issuer
	Submitted straight to authorization				
	Issuer	N/A	7	Yes	Acquirer

<sup>75</sup> There is no low value exemption indicator in 3DS for the Acquirer to request this exemption, however the Issuer can choose to apply this exemption in which case an ECI 05 is returned without a challenge.

<sup>76</sup> This exemption can only be applied by the Issuer – but the indicator can be set by the Acquirer to indicate this exemption may apply.

<sup>77</sup> The trusted beneficiaries exemption indicator in EMV 3DS is only supported in version 2.2 or higher.

**Table 23 Summary of EMV 3DS and Field 34 indicators for Visa Delegated Authentication Program and Resilience and associated fraud liability**

Indicator	Authentication		Authorization	Fraud liability under Visa Rules <sup>72</sup>
	Merchant populated Exemption indicator in EMV 3DS Yes or No	ECI Value	Acquirer populated exemption indicator in authorization F34 Yes or No	
Visa Delegated Authentication Program <sup>78</sup>	Issuer generated CAVV, or Visa generated CAVV or TAVV			
	Yes	7	Yes	Acquirer
Acceptance environment outage Indicator <sup>79</sup>	Submitted straight to authorization <sup>80</sup>			
	N/A	7	Yes	Acquirer

**Table 24: Use of 3DS and Application of Liabilities for out of scope transactions**

Out of scope use case	Submitted Via 3DS	Challenge Applied	Fraud Liability under Visa Rules
Merchant Initiated Transaction (MIT)	No (subsequent transaction)	No	Acquirer ECI 07
	Yes (only for MITs using the Reauthorization indicator that carries a CAVV and associated ECI 05 – generally obtained at CIT)	Yes (however exemption may be applicable)	Issuer ECI 05
Anonymous cards	Yes	No	Acquirer ECI 07 or Issuer ECI 05 <sup>81</sup>
	No	No	Acquirer ECI 07
MOTO	No	No	Acquirer ECI blank, 1, or 4
One-leg-out	Yes	Optional	Issuer ECI 05
	No	N/A	Acquirer ECI 07

<sup>78</sup> The VDA programme is only available in EMV 3DS version 2.2 or higher (not supported EMV 3DS 2.1).

<sup>79</sup> Available from January 2021 Business Release.

<sup>80</sup> Authentication via 3DS has been attempted but due to an outage in the acceptance domain (i.e. in the authentication flow between the merchant, gateway 3-D Secure (3DS) server, and Directory Server) an authentication request was not possible and/or an authentication response could not be received.

<sup>81</sup> An ECI 07 is for the scenario when the anonymous card is not enrolled in 3DS. If the Issuer chooses to support 3DS on Anonymous cards (which is the Visa recommendation as the Visa Attempts Server will not stand in for Anonymous Cards) then the Issuer may authenticate and provide an ECI 05.

## 4.5 Additional guidance on application of the exemptions

This section provides additional practical advice to Issuers, Acquirers and merchants on important considerations and factors to take into account when developing strategies to apply exemptions. For guidance on the order in which to consider applying the exemptions please refer to section 4.3.3.5

### 4.5.1 The low value exemption



Remote transactions up to and including €30 do not require SCA so long as the cumulative number of previous remote transactions using the exemption does not exceed five or the cumulative value of previous remote transactions using the exemption does not exceed €100, since the last application of SCA. Issuers should select either the cumulative or consecutive limit. If Issuers do not select a limit, they must apply both limits on a per transaction basis.

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 should only be used when the transaction does not qualify for the TRA exemption, 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 for transactions submitted via 3DS requires a real-time link between the ACS and the Issuer's Authorization system to check cumulative transaction and value limits have not been breached before applying the exemption.

Issuers also need to ensure:

- They have velocity checking against the cumulative low value transaction count or amount limits in place and that if they are applying the exemption to transactions submitted via 3DS, the Issuer's ACS is linked in real time to the velocity checking in the Issuer's authorization system. If this is not done, there is a risk that the Issuer will apply the exemption at authentication, but when the transaction is submitted for authorization, if the count or value limit has been exceeded, an SCA decline code will be sent prompting the merchant to resubmit the transaction via 3DS for a second time.
- The authorization system is able to increment and reset the velocity counters correctly based when a Low Value exemption and/or RBA and is applied.
- The low value exemption should not be applied to and the cumulative transaction count should not be incremented for account verification transactions that do not require SCA. See Section 4.7.3.2 for more information on these transactions. They are able to apply SCA to a low value transaction when the cumulative transaction count or amount limit is breached and when no other exemption is applicable.
- They are able to provide an SCA decline code should the maximum value or transaction count be exceeded.
- They still apply RBA to low value transactions as required by the PSD2 regulation and should apply SCA if the transaction is perceived to be at risk of fraud.



- The low value transaction limits can be applied separately to different devices/tokens linked to the same payment account<sup>82</sup>.

Issuers should note that:

- Transactions should also not be considered low risk just because they are of low value. Any fraud that occurs will impact the ability of PSPs to apply the TRA exemption.
- The Issuer authorization system can keep track of transactions that have had authentication applied by checking the authentication method value in Field 126.20<sup>83</sup> of the authorization request message.
- However, if the Issuer decides to apply a low value exemption and not to apply SCA to a transaction, it will proceed as ECI 05 with Issuer liability. An Issuer using CAVV Version 7 may choose to use one of five Issuer defined authentication method indicators in the CAVV. This could be used to notify the Issuer host environment that the low value exemption has already been applied in 3DS. Please see *Visa Secure Cardholder Authentication Verification Value (CAVV) Guide* for details.

## 4.5.2 The TRA exemption



### 4.5.2.1 Introduction

TRA is key to delivering frictionless payment experiences for low-risk transactions.

The TRA exemption may be applied by the Issuer or the Acquirer. The process for applying the exemption is summarized in Section 4.3. This section provides some additional information to help Issuers, Acquirers and merchants to manage their strategies for the most effective application of the TRA exemption.

### 4.5.2.2 Requirements Regarding Risk and Transaction Monitoring

The PSD2 SCA RTS lay down minimum requirements for the scope of transaction risk monitoring that must be carried out by PSPs<sup>84</sup>. However, to use the TRA exemption the PSP must take into account a number of additional risk-based factors set out in SCA RTS article 18 and determine, according to the rules in SCA RTS, that the transaction poses a low level of risk.

Visa requirements for the deployment of RBA and EMV 3DS specifications for the data elements that should be provided as the basis for RBA risk scoring are summarized in Section 3.3.10 and the *Visa Secure Program Guide*. Visa has also recommended standards for transaction monitoring and fraud detection and has best practice guides available on these subjects.

Issuers, merchants and Acquirers should ensure that their ACS and Risk monitoring and scoring systems used as the basis of for the application of transaction risk analysis meet these requirements.

<sup>82</sup> SEE EBA Q&A 4036 & 4038 for more information.

<sup>83</sup> See Section 3.2.6 for more detail on Field 126.20 and the list of authentication method indicator values.

<sup>84</sup> See Recital 14 and article 2 of the Regulatory Technical Standards.

### 4.5.2.3 Outsourcing the application of TRA

Issuers will normally utilize risk engines provided by their ACS providers to apply TRA for the purposes of the TRA exemption.

Under the regulation, Acquirers may contractually outsource the application of TRA to merchants however it is still the relevant PSP's fraud rate (and not the merchant's own fraud rate) which must be considered.<sup>85</sup>

### 4.5.2.4 Qualification to apply the TRA exemption

To qualify to apply the TRA exemption, a PSP must maintain its fraud rate within the following reference fraud rates:

**Table 25: Reference fraud rates**

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

The reference fraud rate requirement only applies to the PSP applying the exemption, 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.

Merchants, Acquirers and Issuers can all apply measures to ensure that they maximize their ability to benefit from the exemption. These include:

- **Merchants:** should ensure that they understand their Acquirer's fraud rate and should consider shopping around for Acquirers who are able to apply the exemption at the transaction value level they seek.
- **Acquirers:** have the flexibility to only allow certain low risk merchants to benefit from the exemption and may use this in order to minimize risk and fraud rates.
- **Issuers:** should carefully monitor fraud rates against the reference fraud rate thresholds to ensure they achieve a balanced application of SCA that enables them to maintain fraud rates within their target level for application of the exemptions while minimizing customer friction. While unnecessary application of SCA may decrease fraud rates, the inconvenience to consumers brings the risk of:
  - Increased transaction abandonment, reducing e-commerce transaction rates and consumers switching to alternative, lower friction payment methods or Issuers.

---

<sup>85</sup> (Reference: EBA: Opinion Paper on the implementation of the RTS on SCA and CSC - June 2018, para 47).

- Breaching the Visa rule limiting transaction abandonment (see section 3.5 for more details).

#### 4.5.2.5 Calculation of fraud rates

The PSD2 regulation<sup>86</sup> requires that:

- The calculation of the fraud rate includes both unauthorized 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 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 transactions (see section 2.3.1 for more information), should not be included in the calculation.
- The fraud rate is calculated on a rolling 90-day basis.
- 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 confirmed<sup>87</sup> 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.

### 4.5.3 Application of the trusted beneficiaries exemption

#### 4.5.3.1 Introduction and principles



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.

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

- 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

<sup>86</sup> 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.

<sup>87</sup> Reference EBA Q&A 2019\_4702 [https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019\\_4702](https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4702).

- 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.

#### 4.5.3.2 Issuer options and obligations



Issuers are not under any obligation to provide their cardholders with a trusted beneficiary capability. However, supporting smooth card transactions with identified trusted merchants provides clear benefits to both cardholders and merchants.

Issuers may still choose to apply SCA to a transaction with a listed merchant, if they consider that transaction at risk of fraud.

An Issuer must not systematically decline a transaction that carries a Visa Trusted Listing indicator<sup>88</sup>

#### 4.5.3.3 Merchant options



A merchant can advise their customers of the benefits of using Trusted Lists and facilitate the addition process through:

- Promoting the benefits to regular customers and advising them of how they can add the merchant to their Trusted List.
- Requesting that an Issuer serve the trusted beneficiaries enrollment option form through an SCA challenge when a customer who has not added the merchant to their list completes a transaction with them.

A merchant that is on a customer's Trusted List, can indicate that it would like an Issuer to apply the trusted beneficiaries exemption to a transaction by using the trusted beneficiaries exemption indicator in 3DS.

<sup>88</sup> See Visa Rules ID #0030618. For more details refer to the *Visa Trusted Listing Program Implementation Guide*.

Merchants also have the ability to request that an Issuer does apply SCA to a transaction from a customer who has listed them. They should do this if they are concerned about the risk of the transaction by submitting that transaction via 3-D Secure.

#### 4.5.3.4 Application of the trusted beneficiaries exemption through Visa Trusted Listing



Visa has developed the capability for customers to speed checkout at preferred digital merchants by adding merchants to their Trusted List. For more details on the Visa Trusted Listing Program, please refer to Section 3.6 and the *Visa Trusted Listing Implementation Guide*.

#### 4.5.3.5 Liability



##### 4.5.3.5.1 Regulatory

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

##### 4.5.3.5.2 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.

## 4.5.4 Interpreting the Secure Corporate Payment Processes and Protocols Exemption:



### 4.5.4.1 Background:

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”. 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 considered a “legal person” 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.

Issuers are therefore encouraged to support the exemption and merchants who process transactions originating from secure corporate purchasing systems or travel management systems should discuss with their Acquirer to determine whether any of their transactions should/could be flagged to their Acquirer with the secure corporate exemption indicator. This enables a transaction to be processed without authentication, so long as the Issuer supports the exemption, and the payer qualifies as a “legal person”.

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.

### 4.5.4.2 Interpreting the exemption

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

#### 4.5.4.2.1 The exemption applies only to payers who are not consumers and are “legal persons”

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.

#### 4.5.4.2.2 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

#### 4.5.4.2.3 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.

#### 4.5.4.2.4 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.

#### 4.5.4.2.5 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:

- 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
- 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
- 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.

#### 4.5.4.3 Considerations for Issuers

Issuers should consider applying the exemption (in line with the further considerations set out below):

- When a transaction is received with the secure corporate exemption indicator or SCP extension. This will be the case when a merchant is indicating the transaction originated from a secure access-controlled corporate purchasing system or corporate travel management system
- When a transaction is initiated by a corporate customer considered a “legal person” using a virtual or lodged card/CTA that qualifies for the exemption even if there is no SCP indicator

Issuers supporting the exemption should work with their ACS vendors to ensure that the SCP field is supported in EMV 3DS and that their authorization system also recognizes the SCP indicator when transactions are submitted direct to authorization.

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

#### 4.5.4.4 Identification and processing of transactions qualifying for the exemption

Qualifying merchants who process transactions originating from secure corporate purchasing systems or travel management systems should discuss with their Acquirer to determine whether any of their transactions qualify to be flagged to their Acquirer using the secure corporate exemption indicator in F34 of the authorization request and, if submitting via 3DS, the EMV 3DS SCP extension. This enables a transaction to be processed without SCA, so long as the Issuer supports the exemption.



## 4.6 Challenge Design Best Practice



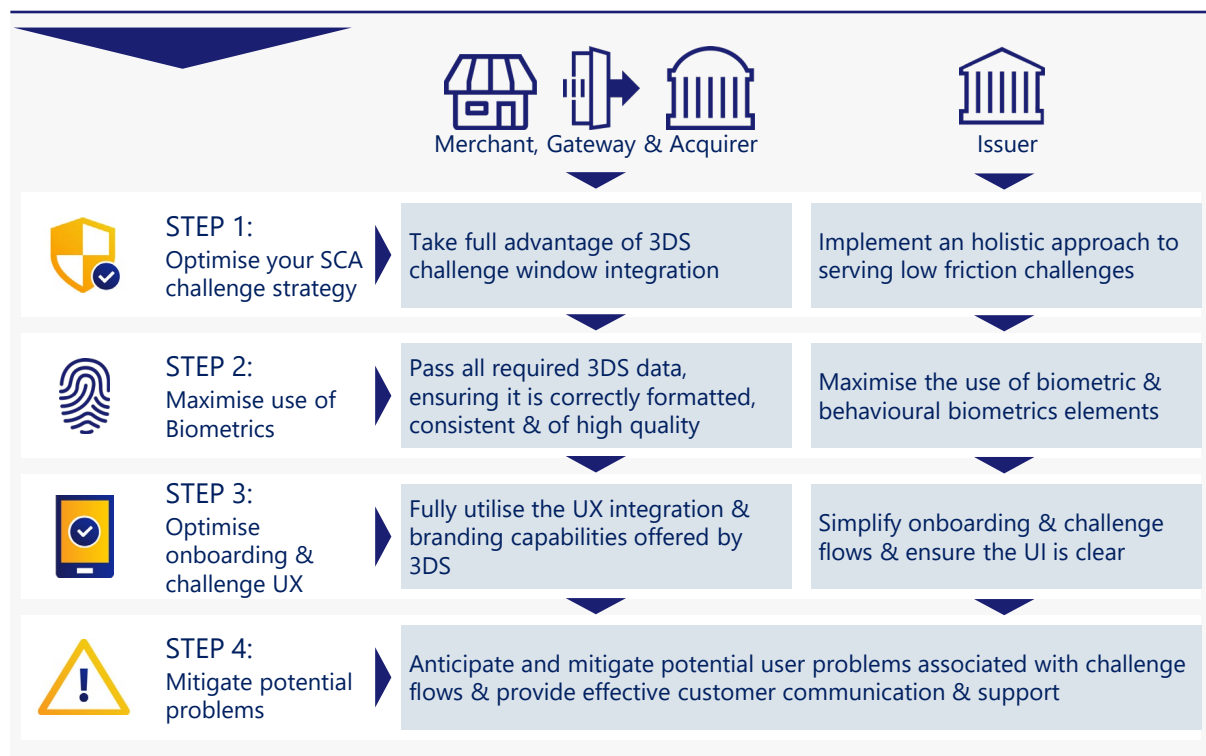
Reducing customer friction is essential to minimising customer dissatisfaction and transaction abandonment.

In those cases where it is necessary to apply an SCA challenge, the impact on customer experience will be minimised through:

- Careful selection and application of SCA factors and elements
- Optimised design of the challenge process and good communication – ensuring customers are clear on what steps they need to take
- Proper integration of the challenge screens into the checkout flow

The key steps to minimising friction are summarised in Figure 22 below

**Figure 22: Minimising friction when SCA is required**



Each of these steps is described in the *PSD2 SCA Challenge Design Best Practice Guide*

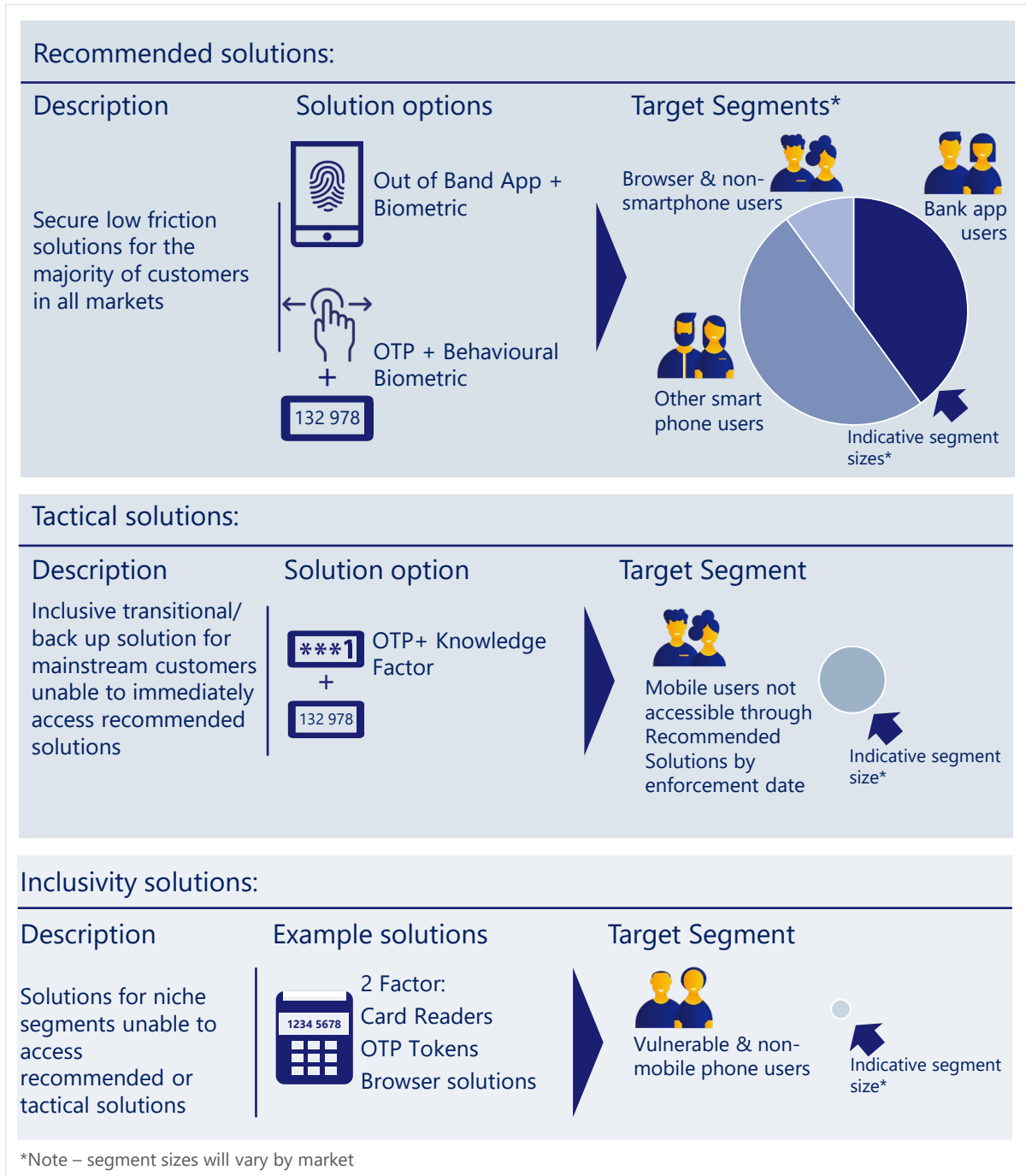
The optimum SCA challenge solution(s) for an Issuer will depend upon the make-up of their customer base. Issuers, ACS and authentication providers should focus on the following SCA Challenge solution options, targeting them at the appropriate target customer segments:

- **Recommended solutions** – secure low friction solutions for the majority of customers in all markets:
  - Out of Band (OOB) app plus biometric
  - OTP plus behavioural biometric
- **Tactical solutions** - Inclusive transitional are back up solutions for mainstream customers unable to immediately access recommended solutions:
  - OTP plus knowledge factor

- **Inclusivity solutions** – for niche segments unable to access recommended or tactical solutions:
  - Two factor card readers, OTP tokens, browser based solutions

The targeting of these solutions at different customer segments is illustrated in Figure 23

**Figure 23 SCA challenge design – the main solution options**



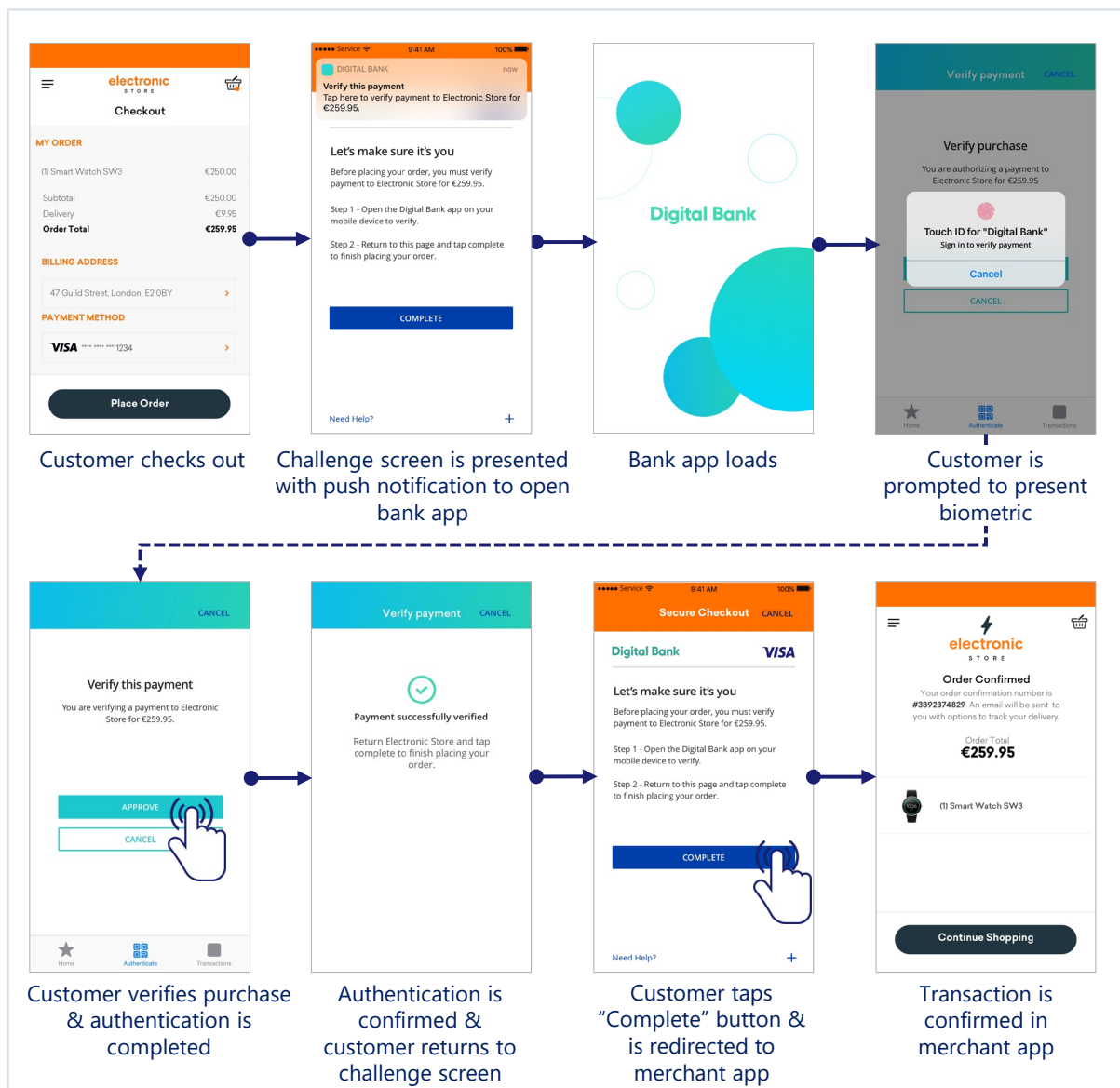
Biometrics are the simplest and securest way to apply SCA. They minimise checkout friction and many customers are familiar with them and find them attractive. Both recommended SCA solutions use biometrics to provide an inherence factor.

#### 4.6.1 Recommended solution 1: Out of Band app plus biometric

Out of Band Authentication allows an existing banking app or dedicated authenticator app to be used to apply SCA.

The app is typically “bound” to the device through a secure onboarding process that includes applying SCA. Once it is securely bound, the app facilitates proof of possession without the need for the user to take steps such as entering an OTP. The app also prompts the customer to complete the authentication process by entering the biometric which will typically be a fingerprint, facial or voice recognition or iris scan. An example user experience of a challenge flow is summarised in Figure 24 below:

**Figure 24: Example user experience flow – native app-based purchase with bank app + biometric authentication**



All Issuers should consider Out of Band app plus biometric as a strategic, long-term solution.

## 4.6.2 Recommended solution 2: OTP plus behavioural biometrics

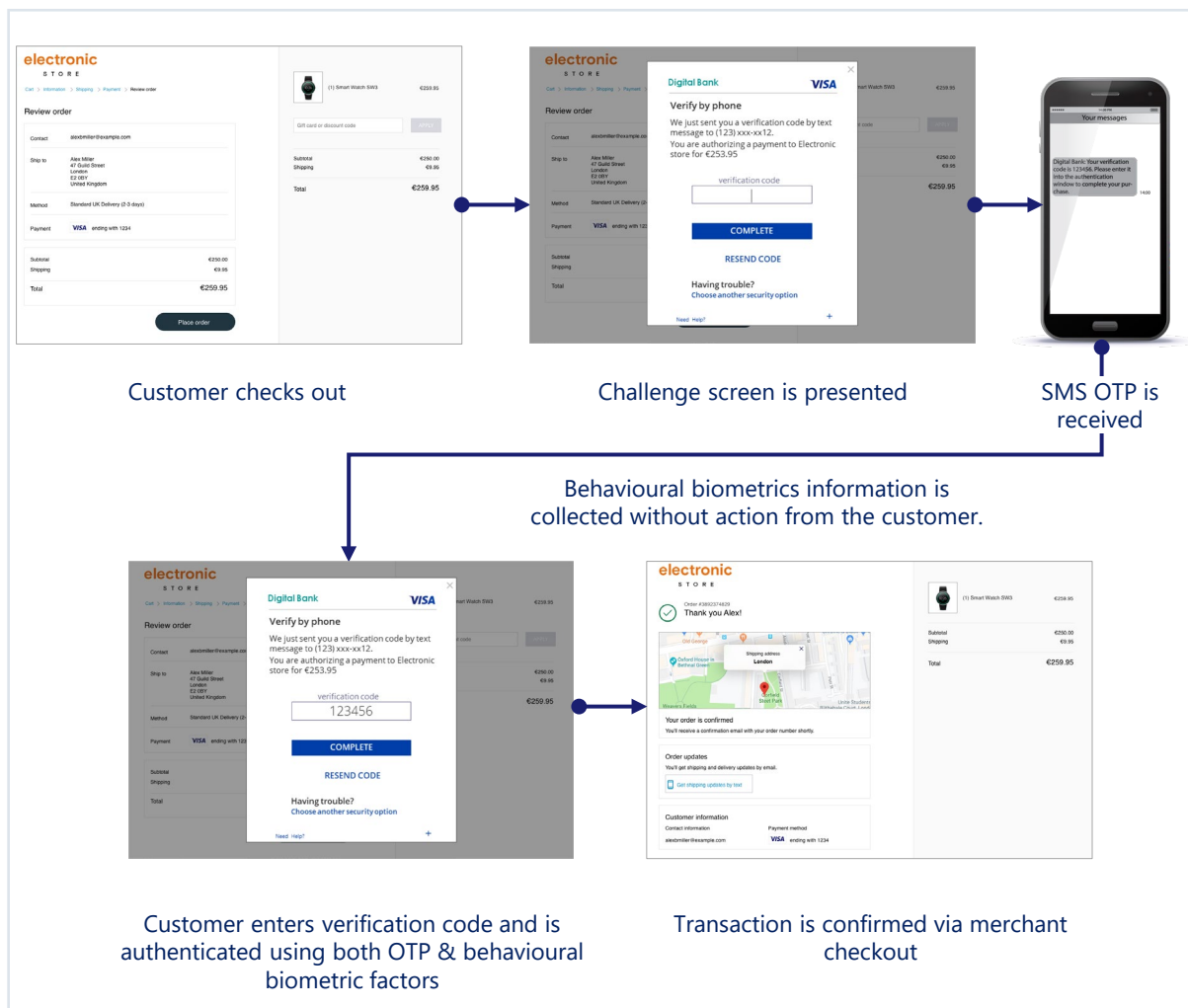
The use of behavioural biometrics is in line with the European Banking Authority opinion on elements for SCA which identifies inherence elements such as keystroke dynamics (identifying a user by the way they type and swipe) and the angle at which the user holds the device.

Behavioural biometrics uses physical behaviour indicators that are unique to an individual customer. These can include the angle at which a device is held, the way keystrokes are entered, gesture analysis and swiping speed.

Indicators are analysed and used to build user profiles and authenticate users.

Behavioural biometrics can be used as a second factor (proving inherence) alongside OTP (proving possession) to provide an SCA solution that is significantly easier for customers to use and far more secure than OTP combined with a knowledge factor. It provides a potentially compliant evolution for existing single factor SMS OTP solutions that delivers the familiar customer experience and is relatively straightforward for Issuers to implement. An example user experience is illustrated in Figure 25 below:

**Figure 25: Example user experience flow – browser-based purchase with SMS OTP plus behavioural biometrics authentication**



For more information on the selection and implementation of these and the alternative tactical and inclusivity solutions please refer to the PSD2 SCA Challenge Design Best Practice Guide. This includes guidance on considerations including:

- The steps that Issuers need to take to optimise the onboarding and challenge user experience for the biometric solutions
- The user experience and security issues associated with use of knowledge factors and the selection of knowledge factors where these need to be used
- The steps that Issuers and merchants need to take to optimise the branding of the 3DS challenge window and its integration into the overall user journey
- The requirement for merchant e-commerce websites to allow JavaScripts to run in the 3DS challenge window so as to enable collection of device data that is critical to ACS risk analysis and the operation of behavioural biometrics based challenge solutions

More detailed information on 3DS UI challenge screen can also be found in section 4 of the EMVCo 3-D Secure Protocol and Core Functions Specification Version 2.2 and additional Visa guidelines for Issuers, ACSs and merchants, including detailed 3DS challenge screen and OOB plus biometrics user experience design guidelines are available on the Visa Developer Center at <https://developer.visa.com/pages/visa-3d-secure>.

## 4.7 Additional Guidelines for Issuers



### 4.7.1 Honoring step-up authentication requests



Issuers must always honor step-up cardholder authentication requests made by merchants to meet SCA requirements. This is particularly important when merchants are requesting a step-up to establish an agreement for future MITs. Refer to Section 5.11.1 of version 2.0 of this guide for more information (however please also read summary guidance provided in section 5 of this version 3.0 before referring to version 2.0).

### 4.7.2 3RI authentication requests



Issuers supporting EMV 3DS 2.1 and above may receive 3RI requests for a new CAVV for a transaction under some of the scenarios defined in Section 5 of version 2.0 of this guide, such as delayed or split shipments. Each 3RI request for a CAVV should be assessed on its merits. Issuers must not blanket decline 3RI requests.

### 4.7.3 Issuer Processing Guidelines



This section summarizes the key points that Issuers need to be aware of when considering their role in the smooth implementation of SCA for e-commerce.

There are a number of important areas for Issuers to consider when processing e-commerce transactions.

#### 4.7.3.1 BIN verification to identify transactions that are out of scope or qualify for an exemption.

Issuers are able to identify whether some transaction types are out of scope of SCA or qualify for an exemption by checking the BIN. This should be the case for:

- Anonymous prepaid cards (out of scope)
- Commercial virtual cards and lodged cards issued to payers who are legal persons and not consumers (these transactions may qualify for the secure corporate payment processes and protocols exemption, subject to the opinion of local regulators).

When Issuers receive transactions that have been sent direct to authorization without the application of SCA and without an out of scope identifier or exemption indicator in Field 34, Issuers should check the BIN of the payment credential in the authorization request to identify whether the transaction is an out of scope anonymous transaction or a transaction to which the secure corporate payments exemption applies. If either of these is the case, the Issuer must not decline the transaction due to lack of SCA or issue an SCA decline code.

#### 4.7.3.2 Account verification transactions

There are a number of reasons why a merchant may perform an account verification transaction as documented in Section 5 of version 2.0 of this guide (however please also read summary guidance provided in section 5 of this version 3.0 before referring to version 2.0) and summarized in Table 26 below. It is important that Issuers understand this is the case and adopt appropriate processing policies as several account verification transactions do not require SCA.

To help Issuers implement policies for these different scenarios, Table 26 below describes various types of use cases where account verification transactions are processed. It summarises how an Issuer can recognize them at a field level and how Issuers should respond. In all scenarios except scenario 6, an Issuer will not be able to determine whether SCA is required or optional based on the data available to them. Visa requests that Issuers rely on Acquirers / merchants to request and provide the CAVV when required and not to decline those transactions with an SCA decline code solely on the basis of the absence of a CAVV.

Note that token-based account verification authorizations that are not identified as MITs will continue to be submitted with a TAVV<sup>89</sup> even if the CAVV is not present.

Account verification transactions should not result in the cumulative transaction count that is used to determine whether the low value transaction exemption can be applied being incremented. See Section 4.5.1 for more information.

#### Best Practice

Some types of zero value transactions do not require SCA. Those types of zero-value transactions should not be declined because no SCA was performed.

---

<sup>89</sup> Token Authentication Verification Value (TAVV). Visa requires TAVV to be present in all token transactions unless the transaction is identified as Merchant Initiated Transaction.

**Table 26: Account verification use cases, associated SCA requirements and expected Issuer processing policies**

#	Merchant Use Case for Account Verification	SCA Required or Optional	Expected Authorization Fields	Expected Issuer Processing Policy
1	<p>To check the validity and/or expiry date of a payment credential</p> <p>This is not a financial transaction (thus out of scope of PSD2), but a transaction processed purely to check the validity of a card.</p> <p>The merchant will check validity and will likely subsequently request a financial authorization including authentication data or suitable exemption indicators.</p>	SCA not required.	<p>Use cases 1, 2 and 3 can all be identified as follows:</p> <ul style="list-style-type: none"> <li>• Zero value</li> <li>• TAVV if token</li> <li>• Field 126.13 will be empty</li> <li>• Field 63.3 will be empty</li> <li>• No initial Transaction ID in Field 125</li> <li>• No MIT indicator in Field 34, Tag 80 Dataset 02</li> <li>• CAVV may or may not be present</li> </ul>	<p>An Issuer will not be able to determine which of these use cases the transaction was processed for; instead it must rely on the Acquirer to provide a CAVV if SCA is required and must not decline using an SCA decline code solely on the basis of no CAVV being present.</p>
2	<p>Setting up an agreement for No-Show, Delayed Charge or Incremental MIT when no initial charge is made at the time the agreement is made.<sup>90</sup></p>	<p>SCA is required (CAVV must be present unless the Secure Corporate Payments (SCP) exemption applies, or the MIT agreement is set up via mail order / telephone order MOTO).</p>		
3	<p>Setting up an agreement for a delayed authorization or split shipment (MIT reauthorization) when no initial payment due at the time the agreement is made.</p>	<p>SCA may be performed but an exemption may also apply<sup>91</sup>.</p> <p>Even if SCA is performed, the CAVV may not be present as it may be kept by the merchant to populate in the MIT reauthorization later for fraud liability protection under the Visa Rules.</p>		
4	<p>Setting up an agreement for a future Unscheduled Credential-on-File (UCOF or usage based on recurring payment) when no initial charge is made at</p>	<p>SCA is required (CAVV must be present).</p>	<p>Use cases 4 and 5 cannot be distinguished, they will both look as follows:</p>	

<sup>90</sup> Note that any of these future MITs must refer to the initial CIT where authentication was performed except if the secure corporate payments exemption was used when setting up the No Show agreement.

<sup>91</sup> See section 3.9.1.3 for details.

#	Merchant Use Case for Account Verification	SCA Required or Optional	Expected Authorization Fields	Expected Issuer Processing Policy
	the time the agreement is made. <sup>90</sup>		<ul style="list-style-type: none"> <li>• Zero value</li> <li>• TAVV if token</li> <li>• "C" in Field 126.13</li> <li>• Field 63.3 will be empty</li> <li>• No initial Tran. ID in Field 125</li> <li>• No MIT indicator in Field 34, Tag 80 Dataset 02</li> <li>• CAVV may or may not be present</li> </ul>	
5	<p>Storing credentials on file for the first time for future CITs when no payment is due at the same time.</p> <p>Note that future CITs performed with the credential will require SCA, or a suitable exemption.</p>	<p>SCA required if risk of fraud which is likely in this case as card details are being provided. (CAVV may not be present in the eventuality that there is no risk of fraud). The Issuer should not decline on the basis of requiring SCA as there is a possibility the merchant may have evaluated no risk of fraud.</p>		
6	<p>Setting up an agreement for a subscription (recurring payment) or installment / prepayment agreement) when no payment is due at the time of the agreement.</p>	<p>SCA is required (CAVV must be present).</p>	<ul style="list-style-type: none"> <li>• Zero value</li> <li>• TAVV if token</li> <li>• "R" or "I" in Field 126.13</li> <li>• Field 63.3 will be empty</li> <li>• No initial Tran. ID in Field 125</li> <li>• No MIT indicator in Field 34, Tag 80 Dataset 02</li> <li>• CAVV must be present</li> </ul>	<p>If the CAVV, or CTF TAVV under Delegated Authentication is not present or valid, then the Issuer must decline with an SCA decline code.</p> <p>This is the only Account Verification use-case where an Issuer can and should request SCA if not present. This is because case 6 is the only use-case where an Issuer can recognize that SCA is necessary.</p>

#### 4.7.3.3 Inclusion of CAVV and TAVV in MIT transactions

MIT transactions submitted after a previous CIT used to establish the agreement do not typically include CAVV or TAVV information, with the exception of Reauthorizations and resubmissions. In the case of Reauthorization, the CAVV may be included by a merchant in order to claim fraud liability protection under Visa Rules (see Section 4.2.4.3).

Resubmissions as used in mass transit use cases where the initial contactless transactions was declined for lack of funds, will not be provided with a CAVV or TAVV as the original CIT to which they refer in the initial Transaction ID field is exempted from PSD2 SCA (for more information refer to Section 5.9 of version 2.0 of this guide, however please also read summary guidance provided in section 5 of this version 3.0 before referring to version 2.0).



#### 4.7.3.4 Reauthorizations

A number of the scenarios in Section 5 of version 2.0 of this guide use the Reauthorization message reason code 3903 with an initial Transaction ID in Field 125 to identify cases where an authorization is being performed when the cardholder is not present to complete a previous transaction, for example in the case of a:

- Delayed authorization; or
- Because multiple authorizations are processed, one for each individual shipment or item of one check out order

The transaction was in scope, but exemptions could apply. The transaction is only treated as an MIT as it could not be completed at the time.<sup>92</sup> Whilst typically, MITs do not include a CAVV, for Reauthorizations due to delay or split shipment, a merchant may optionally choose to include a CAVV for fraud liability protection.

To include a CAVV the merchant must either:

- Obtain one during an earlier interaction where an account verification transaction was performed but the CAVV was kept for this later authorization (e.g. when a delayed order was placed) or;
- Obtain a new one by calling the 3RI feature of 3DS just prior to the delayed authorization or split shipment authorization<sup>93</sup>

The merchant may decide not to include a CAVV when either a valid exemption was used during the initial authorization and thus no CAVV was obtained, or when the merchant has already used the CAVV in an initial authorization and has not called 3RI to obtain a new one.

If there is no CAVV, the Issuer may not decline with an SCA decline code, since the cardholder is not available for authentication and the initial authorization was authenticated or exempted.

For token transactions, as Reauthorizations are flagged under the Visa MIT Framework, no TAVV will be included.

##### 4.7.3.4.1 Expired CAVVs

It is important to note that merchants submitting Reauthorizations (MRC 3903) relating to delayed or split shipments may, on occasion include a CAVV that is over 90 days old. Visa Rules clearly state that fraud liability protection is limited to 90 days and therefore Issuers have dispute rights for any such transactions they receive. However, the CAVV if otherwise valid, provides evidence that SCA was performed as part of the CIT. Issuers should not decline transactions based on the CAVV being more than 90 days old.

---

<sup>92</sup> Such an MIT is not out of scope of SCA but is instead the completion of a transaction where either SCA or an exemption applied.

<sup>93</sup> If 3RI is not yet available, the original CAVV may be used as an interim up to a maximum of five times – note that liability protection is in this case limited to the 90 days validity of the CAVV. Note: This interim arrangement can only be applied until 01 Sept 2022.

### Key Point

Under Visa rules, merchants are liable for fraud on reauthorizations including a CAVV that is over 90 days old. However, the CAVV can still be used as evidence that SCA was performed and Issuers should not decline due to the age of the CAVV.

CAVVs over a year old will fail validation by Visa and will be flagged accordingly.

#### 4.7.3.5 Transactions identified in accordance with the MIT framework

Issuers can identify MITs using one of the following methods:

- The existing Visa MIT Framework, or
- The new initiating party indicator in Field 34<sup>94</sup>. The Acquirer must continue to use the existing Visa MIT Framework to indicate MITs. When receiving transactions that are indicated as MITs using the framework, Visa will automatically populate the value of "1" in Field 34 (Tag 80, Dataset ID 02). This enables Issuers to recognize a transaction as an MIT (and therefore out of scope of PSD2 SCA) by simply checking for the value of "1" in that tag.

Transactions identified as MITs will have been performed at a time when the cardholder is not available. For this reason, Issuers must not decline a transaction flagged as an MIT solely on the basis that cardholder authentication was not performed (i.e. Issuers may not decline a transaction flagged according to the MIT framework based on the lack of authentication data).

### Best Practice

Issuers must not decline MITs on the basis that authentication is required (SCA decline code), as the cardholder is not present to authenticate.

For more information about how to recognize the different types of MIT, how they are indicated in authorization messages to distinguish them from CITs, Issuers should refer to Section 3.9.3.

Issuers are also reminded they must not decline a transaction based solely on a missing CVV2 for transactions where it is prohibited or not required to capture the CVV2: in Visa's view, all MITs fall in this category. For more details, including other transactions that cannot be declined solely on the basis of a missing CVV2, please refer to Visa Rule ID# 0029985 and 0029600.

---

<sup>94</sup> For more information please refer to *Article 9.1.4 of the October 2019 and January 2020 VisaNet Business Enhancements Global Technical Letter and Implementation Guide, Effective: 5 September 2019.*

#### 4.7.3.6 Evaluate each transaction on its merits

Issuers are reminded that they are required, according to Visa rule # 0029326 to evaluate each transaction on its own merits. This means Issuers must not block, refuse, or decline Authorization Requests, payment token provisioning requests, or Transactions in a systematic or wholesale manner, unless there is an immediate fraud threat, or an exception is otherwise specified by applicable laws or regulations or in the Visa Rules.

#### 4.7.3.7 Authentication provided by parties other than the merchant

In some cases, authentication may be requested by a party other than the merchant submitting authorization. Therefore, Issuers must be aware that the merchant name used in authentication may legitimately be different to the merchant name in the authorization and process accordingly. In such instances it is best practice for the authenticating party to include the end merchant name in the authentication request. For example, an Online Travel Agent should authenticate on behalf of the merchants they represent citing the merchant name as "Online Travel Agent name \* merchant name".

#### 4.7.3.8 Using TAVVs to prove cardholder authentication

In some cases, qualifying token requestors will be able to use the new Cloud Token Framework (CTF) TAVV format as evidence that cardholder authentication has been performed. In such cases a CAVV is not required for SCA compliance. TAVVs used in this way do not currently qualify the merchant for fraud liability protection. Further information on the Visa Token Service will be made available as these new options become available.

Visa requires a TAVV (existing or new CTF TAVV) to be present in all token transactions unless the transaction is identified as an MIT.

#### 4.7.3.9 Making allowances for legitimate data variations

Issuers need to be careful not to be overly prescriptive when matching data between authentications and authorizations, or CITs and the subsequent MITs. For example:

- The merchant name may be different between the authentication and corresponding authorization
- The merchant name may be different between a CIT and subsequent MITs (see Section 5.16.1 of version 2.0 of this guide, however please also read summary guidance provided section 5 of this version 3.0 before referring to version 2.0)
- The merchant name may differ for other reasons. For example, if the merchant uses multiple Acquirers, each of whom populate the merchant name slightly differently
- The transaction amount may vary. For example:
  - A holiday booking fulfilled by more than one merchant may have been authenticated for the full amount of the booking but each individual merchant may request a separate authorization for a lower amount corresponding to the value of their part of the booking.
  - In the case of a split shipment, the merchant may request separate authorizations for the value of each stage of the shipment. If 3RI is not yet available, the original CAVV may be used as an interim up to a maximum of

five times and in each authorization request the amount will be lower than amount of the original CAVV.<sup>95</sup>

#### 4.7.3.10 Handling transactions from merchants who are not yet fully ready for PSD2

Issuers are reminded that to assist merchant who are not ready to ready to send a valid Tran ID in MITs, Visa has assigned Tran IDs to Acquirers for use in this field and will continue to do so for an interim period of time. In those cases, Issuers will see a value of “0100000000000000” in Field 125 instead of the transaction ID of the original CIT or a transaction ID of a previous transaction in the agreed MITs. Issuers are asked to accept this value for an interim period of time. Refer to section 3.9.3 for more details.

All transactions from the travel and hospitality sector within scope of the SCA regulation must be compliant by the national regulatory enforcement date. Use of the MOTO indicator for some of these transactions<sup>96</sup> will be available as an interim solution to a technical issue preventing merchants from being able to provide all required proof of authentication / reference to MIT mandate setup authorization in their transaction flagging.

Issuers should continue to perform risk-based analysis on any MOTO transactions before making an authorization decision. It is possible that some of the transactions currently key-entered without any MOTO indicator may not be upgraded to include the MOTO indicator in time for the regulatory enforcement date. These transactions may look in-scope and without any authentication; Issuers will need to consider which authorization decision to take in those circumstances.

## 4.8 EMV 3DS and authorization fall-back options



If for any reason an Issuer is unable to authenticate a transaction using EMV 3DS, or is unable to respond to an authorization request, Visa will step in, where applicable, through the application of the Visa Attempts Server or Stand-in Processing Service (STIP) respectively.

### 4.8.1 The Visa Attempts Server

The Visa attempts server will respond to an authentication request if the Issuer does not support EMV 3DS 2.1, or when a transaction is submitted using a version of 3DS that the Issuer supports<sup>97</sup> but Issuer the Issuer’s ACS is unavailable or does not respond in time<sup>98</sup>. In these cases, the Attempts Server will respond with an ECI 06 and the Issuer assumes liability. The Issuer may still authorize or decline the transaction at authorization.

Issuers should note that ECI 06 transactions have not been subjected to SCA. Once SCA is actively enforced by the NCA most, if not all, Issuers will be live on EMV 3DS 2.1 so the only ECI 06s should be because of ACS timeouts. Issuers will need to decide whether they can justify

<sup>95</sup> The interim arrangement only applies until 01 Sept 2022.

<sup>96</sup> This is limited to out of scope MIT transactions in certain MCC codes, where authentication has been performed by a third party agent at the time of booking to set up the MIT mandate.

<sup>97</sup> Note if a transaction is submitted using EMV 3DS2.2 or above and that version of 3DS is not supported by the Issuer, the Visa Attempts Server will not stand in.

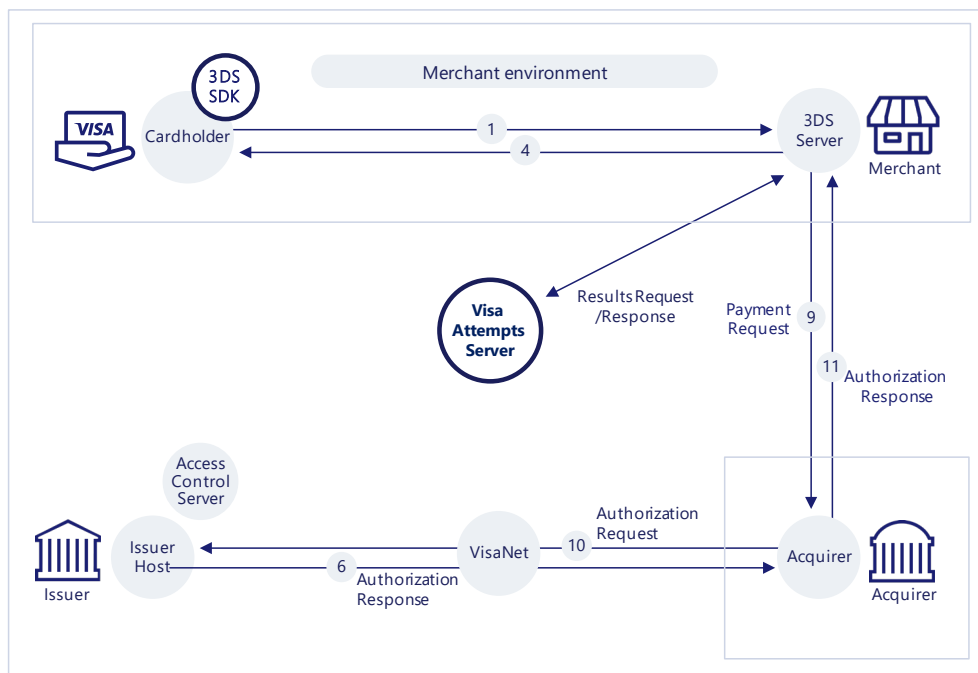
<sup>98</sup> Some card ranges and message types are excluded from attempts processing. See *the Visa Secure Program Guide* for further information.

approving these transactions with their NCA (i.e. exceptional outage) or consider applying the Issuer TRA or low value exemption if the transaction qualifies.

Issuers are advised to review their management of ECI 06 authorization responses should the Issuer's ACS be unavailable to respond to an authentication request once regulatory enforcement is in effect. Issuers may also want to consider their business continuity plans, in order to minimize the impact on consumers while ensuring that regulatory requirements are met.

The processing fee for each transaction processed by the AACS will be USD 0.075.

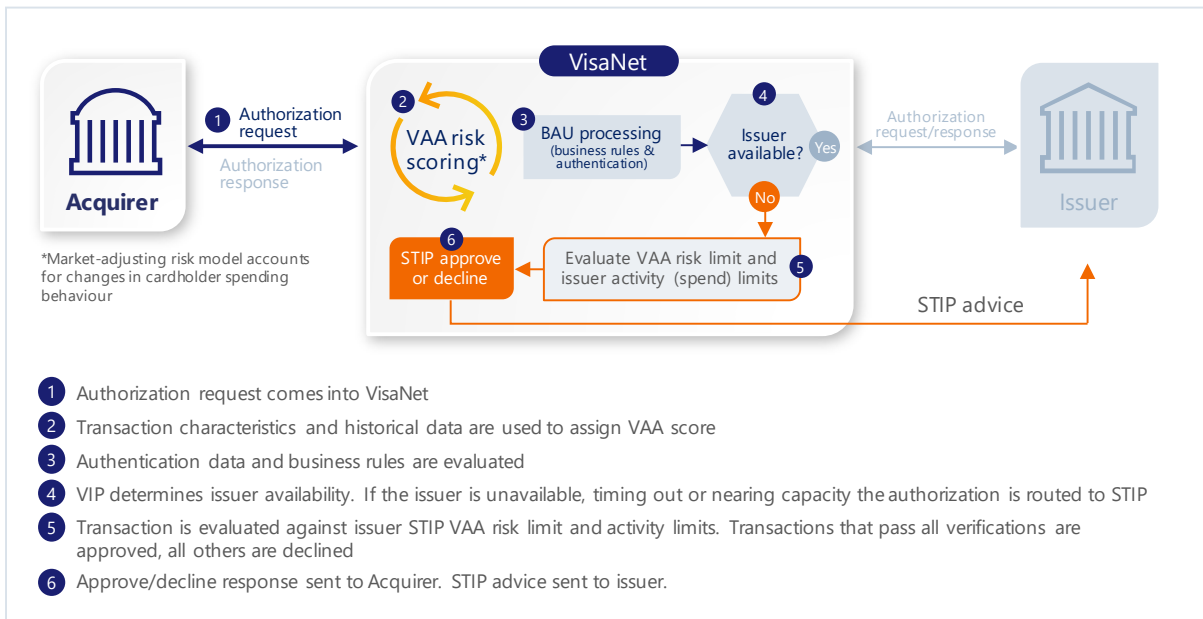
**Figure 26: The role of the Visa Attempts Server**



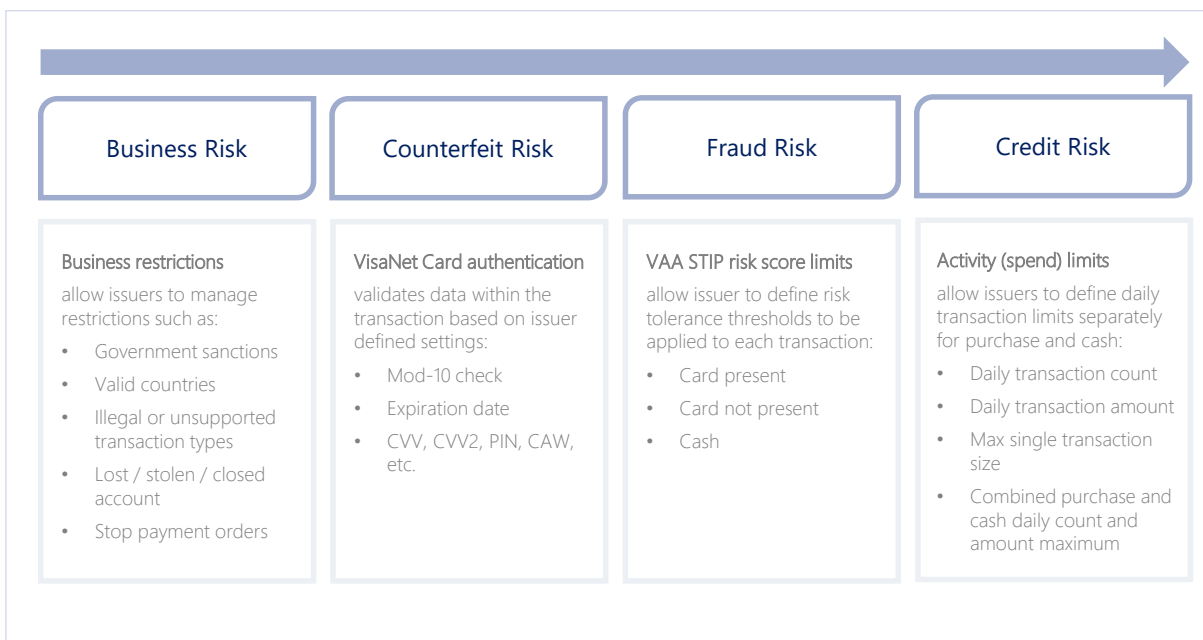
#### 4.8.2 STIP

Stand-in processing (STIP) occurs when Visa acts as a backup processor that approves or declines authorizations on behalf of an Issuer. The VisaNet Integrated Payment (V.I.P.) System determines when a transaction is eligible for STIP based on Issuer availability or participation in various Visa on-behalf-of services. When a transaction is routed to STIP, a series of Issuer-defined parameters and activity limits are used to determine how the transaction should be processed.

**Figure 27: Operation of the STIP approval service**



**Figure 28: The VisaNet STIP service offers a robust set of parameters to effectively manage STIP risk, including:**



Please note: it is extremely important that Issuers provide Visa with their CAVV keys otherwise all e-commerce transactions will be declined in VisaNet STIP irrespective of what options have been set for SCA.

Activity limits determine the number of transactions and the amount that can be approved per day. The Visa Advanced Authorization (VAA) Score evaluates the fraud risk for each transaction.

**Figure 28: An example set of STIP Limits for an Issuer's BIN**

Parameter	VAA Score Threshold	Total Count	Total Amount	Max Single Tran
Purchase-Card Present	30	10	\$1,000	\$500
Purchase-Card Not Present	30			
Cash	30	2	\$500	\$300
Max Combined		10	\$1,000	N/A

**VAA Limits**

- Card present, Card not present & Cash

**Activity Limits**

- Purchase & Cash
- Count & Amount
- Maximum single transaction amount

**Combined Maximums (Purchase & Cash)**

- Combined transaction count
- Combined transaction amount

Parameter	VAA Score Threshold	Total Count	Total Amount	Max Single Tran
Purchase-Card Present	30	10	\$1,000	\$500
Purchase-Card Not Present	30			
Cash	30	2	\$500	\$300
Max Combined		10	\$1,000	N/A

**Figure 29: VisaNet STIP protects an Issuer's business**

- ✓ It supports different limits for debit and credit portfolios for both purchase and cash transactions.

✓ Issuers should review and update limits regularly in order to create a seamless customer experience.

✓ Every transaction is allocated a risk score, irrespective of whether the issuer subscribes to Visa Advanced Authorization or Visa Risk Manager. Visa will decline all transactions in STIP that are above the risk threshold accepted by an issuer.

✓ It can perform cardholder validation and checks on behalf of issuers.
- ✓ Issuers can identify and manage customers that require special treatment. Important customers can be treated differently, and any reported lost or stolen cards will not be approved in STIP.

✓ Having STIP limits in place can allow issuers to focus on fixing the underlying problem rather than handling calls from unhappy customers when the unexpected happens.

#### 4.8.2.1 Strong Customer Authentication Parameters for STIP<sup>99</sup>

To ensure that STIP transactions support the PSD2 requirement to enable SCA, SCA STIP parameters are available for Issuers in the European Economic Area (EEA) in the following scenarios:

- Does the issuing Bank Identification Number (BIN) want to decline all ECI 06 e-commerce transactions without a valid exemption in STIP?
- Does the issuing BIN want to decline all ECI 07 e-commerce transactions without a CAVV and without a valid exemption in STIP?
- Does the issuing BIN want to decline all ECI 07 e-commerce transactions with a CAVV and without a valid exemption in STIP?

The default value for all three questions listed above is 'No'. For example, an ECI 06 e-commerce transaction without a valid exemption will not be declined in STIP due to SCA.

<sup>99</sup> These requirements are defined in VBN: Changes to Stand-In Processing to Support Strong Customer Authentication Under PSD2 18<sup>th</sup> April 2019.

Issuers that choose to participate in these SCA STIP options must submit the SCA Client Implementation Questionnaire (CIQ) to specify their SCA parameters for STIP.

Note: Under the Visa Rules, the Issuer is responsible for a transaction authorized by STIP, including where the Issuer does not change the default values (via the CIQ) as listed above.

Issuers can define the response code to be used in SCA STIP for each of the three questions above:

- Declined with Response Code 05—Do Not Honor
- SCA decline code: Resubmit with SCA applied
- Approved with Response Code 00 (Note: This is the default if the Issuer does not use the STIP options as listed above.)

Issuers can define the exemptions to be used in SCA STIP; the valid exemptions from SCA for are below:

- Low value payment
- Transaction Risk Analysis (TRA)
- Trusted merchant / beneficiary
- Secure corporate payment

Issuers may also define that delegated authentication is applied.

Additionally, Issuers can choose to select an exemption for transaction amounts less than the low value limit (EUR 30).

The default values for all six exemptions listed above will be 'No'. For example, a transaction may qualify for a TRA exemption, but will be declined by default unless Issuers specify their SCA STIP parameters by submitting the SCA CIQ.

#### 4.8.2.2 Scope of SCA / PSD2 for STIP Transactions

In addition to the exemptions listed above, several types of transactions are out of scope for, or do not require SCA checks in STIP. These include:

- MITs
- MOTO transactions
- Original Credit Transactions (OCTs)
- One-leg-out transactions

For STIP to recognize MITs as out of scope, a transaction needs to be flagged with the indicators from the existing MIT framework. For more details, refer to Section 3.9.



## 4.9 Visa Direct and SCA under PSD2



### 4.9.1 Background

Visa Direct is a real-time push payment platform designed to facilitate real-time payments to accounts globally. Visa Direct enables person to person (P2P) payments and can also be used by companies and public institutions for funds disbursements (e.g. insurance, salary, or benefit payments).

Visa direct can be used for a number of use cases including, for example:

**Table 27 Visa Direct Use Cases**

Money Transfer Use Cases	Funds Disbursement Use Cases
<ul style="list-style-type: none"><li>• P2P money transfer via bank or third-party apps</li><li>• Loading money into another payment account, for example a prepaid card, e-money or stored value account</li><li>• Withdrawal of money from another payment account, for example a prepaid card, e-money account</li></ul>	<ul style="list-style-type: none"><li>• General funds disbursements, for example, online gambling pay outs, lottery pay outs, shared economy</li><li>• Merchant initiated disbursement, for example an insurance claim pay out</li><li>• Government initiated disbursement, for example VAT tax refunds</li></ul>

### 4.9.2 Visa Direct Transaction Types

Transactions associated with the Visa Direct service fall into two categories:

- Original Credit Transactions (OCTs); used to “push” funds to a Visa cardholder’s account

Account Funding Transactions (AFTs); used to “pull” funds from a Visa cardholder’s account

These transaction types are defined below:

#### 4.9.2.1 Visa Direct Original Credit Transactions (OCTs)

Original Credit Transactions (OCTs) are push payments that allow a Visa cardholder to receive funds to their eligible Visa card account in near-real time.

Examples of OCTs are:

- A B2C payment such as the pay out of an insurance claim to a customer’s Visa card account or a salary payment made by a ride sharing platform to a driver.
- Small B2B supplier payment for business related supplies
- A gambling merchant paying winnings to a customer’s Visa card

OCTs may be initiated by a Visa member Acquirer on behalf of:

- A corporate entity who is paying a customer using a secure payment process or protocol (for example an insurance pay out)
- A business with a need to pay a consumer on their Visa card

OCTs can be identified by Authorization Field 3, Field Value 26.

#### 4.9.2.2 Account Funding Transactions (AFTs)

Account Funding Transactions (AFTs) are transactions used to pull funds from a Visa card account for the purpose of funding a different, non-merchant account; for example, loading or topping up prepaid card accounts, moving funds into another financial account such as a bank or E-money account, acting as a funding source for person-to-person (P2P) money transfers, or loading third-party staged digital wallets.

Examples of AFTs include:

- Consumer funding a P2P money transfer
- Consumer loading funds into an e-money or other stored value account
- Consumer loading funds onto, or topping up a prepaid payment card

AFTs are processed e-commerce transactions identified by Field Value 10 in Authorization Field 3.

Other purchase transactions are identified by Field Value 00 in Authorization Field 3.

#### 4.9.2.3 AFT and OCT transactions

An AFT may precede an OCT transaction, for example when funds are pulled from a payer's Visa card account (an AFT) to fund a P2P money transfer destined to a recipient's Visa card account (an OCT).

#### 4.9.3 The Application of PSD2 SCA and exemptions to Visa Direct Transactions

Visa Direct AFT transactions are in scope of PSD2 SCA and SCA must be applied unless an exemption applies, or the transaction is out of scope. For example, this may be the case where the customer is loading funds into an account with a service provider they have added to a Trusted List and the trusted beneficiaries exemption may apply.

Examples include:

- Consumer funding a P2P money transfer
- Consumer loading funds into an e-money or wallet account
- Consumer loading funds onto, or topping up a prepaid payment card

The SCA requirement applies to payers, and therefore SCA does not need to be applied by the recipient when they receive an OCT transaction.

Examples include receipt of:

- Refunds
- Insurance claim Pay outs
- Other funds disbursements

Additional practical guidance on the application of SCA to Visa Direct transactions and the identification of Visa transactions that do not require SCA is given in Section 5.14 of version 2.0 of this guide (however please also read summary guidance provided in section 5 of this version 3.0 before referring to version 2.0).

#### 4.10 Visa Secure Remote Commerce/Click to Pay



Click to Pay with Visa has launched as part of a wider industry initiative in accordance with the Secure Remote Commerce specifications published by EMVCo.

Merchants who use Click to Pay with Visa to provide a smoother checkout experience for their customers should be aware that using it alone does not fulfil their SCA obligations. Once the merchant has been provided with the payment credentials by Click to Pay, authentication must still be sought (e.g. using 3DS) or a suitable exemption exercised.

The information above also applies to Visa Checkout merchants who have not yet been migrated to Click to Pay with Visa.

#### 4.11 Visa Secure Authentication Technology and non-Visa Transactions

To maintain Visa Secure interoperability, any e-commerce transaction authenticated using the Visa Secure authentication technology must facilitate a Visa transaction. Entities that wish to use Visa Secure technology for non-Visa transactions, for example submitting a non-Visa transaction for 3DS authentication via the Visa Directory Server, must receive prior written permission from Visa. The Visa Rules have been updated to reflect these requirements. Clients that are currently using Visa Secure technologies to authenticate non-Visa transactions should contact their Visa Account Executive to discuss next steps<sup>100</sup>.

---

<sup>100</sup> See *Visa Business News: Updated Rules for Visa Secure Authentication Technology* 9 May 2019.



## 5. Payment use cases and sector specific guidance for merchants and PSPs

---

This section provides merchants and Acquirers with best practice examples of how to ensure SCA is performed across common e-commerce payment scenarios, including MITs. This guidance is currently under review following EBA clarification that in payment use cases where the final amount is unknown, transactions must be reauthenticated if the amount increases above the amount initially authenticated.

A revised version of this guidance taking account of this clarification will be included the next version (Version 4.0) of this guide.

In the meantime, merchants, Acquirers and Issuers seeking guidance on performing SCA in specific payment use case scenarios should still refer to version 2.0 of this guide but should take into account that the guidance given in Version 2.0 that states that in Visa's view it is permissible for the amount in authentication and authorization to vary within the customer's reasonable expectations (but by no more than 15% as required by Visa's rules), is no longer valid and is instead replaced by the guidance provided in this version 3 of the guide in section 4.2.2.3.

Please note that in the UK, discussions are underway with the UK Financial Conduct Authority regarding the allowance of a reasonable variation to authorization amounts. Until discussions conclude, Visa will not prevent UK merchants from continuing to clear up to 15% greater than they authorized / authenticated (although Issuers and Acquirers will need to make their own decisions regarding such transactions). However, as of 17 October 2020, all UK e-commerce merchants are permitted the same flexibility as EEA merchants to use initial / estimated and incremental authorizations as described in section 4.2.2.3.

## 6. Bibliography

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

**Table 28: Bibliography**

Document/Resource	Version/Date	Description
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 SCA Regulatory Guide	December 2020	Summarises 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.
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.
PSD2 SCA Commercial Cards Guide	Forthcoming	Summarises considerations for meeting the requirements of PSD2 SCA for Issuers of commercial card products
PSD2 SCA Secure Corporate Payments Exemption Implementation Guide	Forthcoming	Provides additional guidance on the use and support of the Secure Corporate Payments exemption.
Visa Delegated Authentication Program Implementation Guide	Version 1.0 5 <sup>th</sup> April 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.

<p>Visa Trusted Listing Program Implementation Guide</p>	<p>Version 1.0 9<sup>th</sup> April 2019</p>	<p>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.</p>
<p>European EMV 3DS 2.2 Implementation Guide</p>	<p>Version 1.0 30 October 2019</p>	<p>Provides a summary of the features, benefits and implementation considerations for EMV 3DS 2.2</p>
<p>PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements</p>	<p>Version 1.0 October 2019</p>	<p>Guide summarizing Visa Rules relevant to the application of PSD2 SCA.</p>
<p>Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure</p>	<p>Version 1.1, 21 August 2019</p>	<p>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:</p>
<p>Visa Secure Issuer Implementation Guide for EMV 3-D Secure</p>	<p>Version 1.1, 21 August 2019</p>	<p>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</p>
<p>Visa Secure Program Guide – Visa Supplemental Requirements</p>	<p>Version 1.1 8<sup>th</sup> August 2019</p>	<p>This document is for Visa Secure and its use to support authentication of payment transactions</p>
<p>Visa Secure Cardholder Authentication Verification Value (CAVV) Guide</p>	<p>Version 3.0 April 2019</p>	<p>Provides detailed information on CAVV creation and verification and use in authorization for both 3DS 1.0 and EMV 3DS.</p>
<p>VisaNet Business Enhancements Global Technical Letter and Implementation Guide.</p>	<p>October 2018 Version 3.0 (Major Release) and January 2019 Version 2.0 (Minor Release) – effective 6 September 2018</p>	<p>Provides VisaNet Acquirers, Issuers, and processors with updates to the technical changes for each business enhancement to VisaNet processing systems and detailed information on implementation, activation, and testing activities.</p>
<p>VisaNet Business Enhancements Global Technical Letter and Implementation Guide.</p>	<p>October 2019 Version 3.0 (Major Release) and January 2020 Version 2.0 (Minor</p>	<p>Provides VisaNet Acquirers, Issuers, and processors with updates to the technical changes for each business enhancement to VisaNet processing systems and detailed information on implementation, activation, and testing activities.</p>

	Release) – effective 5 September 2019	
Visa Merchant Purchase Inquiry (VMPI) information on the Visa Developer Center	N/A	Additional information on the service and the API <a href="https://developer.visa.com/capabilities/vmpi">https://developer.visa.com/capabilities/vmpi</a>
Visa Biometrics information on the Visa Developer Center	N/A	Additional information on the service and the API <a href="https://developer.visa.com/capabilities/biometrics">https://developer.visa.com/capabilities/biometrics</a>
Visa Technology Partner Portal	N/A	Portal with additional resources including details on EMV 3DS available at: <a href="https://technologypartner.visa.com/Library/3DSecure2.aspx">https://technologypartner.visa.com/Library/3DSecure2.aspx</a>
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
3DS Performance Rules FAQ		Summarizes Visa Performance Program rules for Issuers and Acquirers
EMVCo 3-D Secure Specification	V2.2	Specification for the core 3DS technology that includes message flows, field values etc. available at: <a href="https://www.emvco.com/emv-technologies/3d-secure/">https://www.emvco.com/emv-technologies/3d-secure/</a>
BASE I Processing Specifications V.I.P. System	Effective: 1 Jun 2019	V.I.P. System BASE I Processing Specifications describes processing requirements and options for the BASE I System within the VisaNet Integrated Payment (V.I.P.) System.
Visa Business News: Important Changes to 3-D Secure Rules to Support Strong Customer Authentication Compliance	5 September 2019	VBN stating Visa requirements for the implementation of EMV 3DS.
Visa Business News: AI10292 Update to CAVV—Exceptions to Reuse in Europe	20 August 2020	VBN explaining CAVV reuse.
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 SCXA enforcement in the EEA.

<p>Visa Business News: Preparing Travel and Hospitality Merchants for SCA Compliance on Indirect Sales Transactions</p>	<p>20 August 2020</p>	<p>VBN outlining travel and hospitality merchants' options for avoiding declines for online booking transactions performed via third parties</p>
<p>Visa Merchant Marketing Communications Guide</p>	<p>September 2019</p>	<p>This guidebook containing advice and communications to help merchants prepare for PSD2 SCA and raise customer awareness of the changes on merchant websites and in-store.</p>



# Glossary

**Table 29: 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.</p> <p>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.
Account Binding	The process of verifying that the merchant or wallet customer is also the Issuer's cardholder by performing Issuer authentication when binding is established. This can occur during token provisioning or as a standalone action. Account binding links a token to the Token Requestor's customer and enables a customer's authentication

Term	Description
	into their merchant or wallet account to be used in the performance of SCA under the Delegated Authentication Program.
Account Funding Transaction (AFT)	A Transaction that transfers funds from an account linked to a Visa cardholder to another account.
Authentication	<ul style="list-style-type: none"> <li>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</li> </ul>
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 response. VisaNet then informs the requestor of the response, who passes the information along to the Merchant.
<b>B</b>	
Bank Identification Number (BIN)	A 6-digit number assigned by Visa and used to identify a Member or VisaNet Processor for Authorization, Clearing, or Settlement processing
BASE I	A component of the V.I.P. System that provides Authorization related services for Transactions that are subsequently cleared and settled through BASE II.
BASE II	A VisaNet system that provides deferred Clearing and Settlement services to Members.
<b>C</b>	
Cardholder Authentication Verification Value (CAVV)	A unique value transmitted in response to an Authentication Request.

Term	Description
Cloud Token Framework	The Cloud Token Framework is an enhancement to the Visa Token Service for e-commerce and card on file tokens bringing the benefits of device based tokens and cardholder verification to all tokens used for e-commerce
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"> <li>• Visa Corporate Card</li> <li>• Visa Business Card</li> <li>• Visa Purchasing Card</li> </ul>
Customer Initiated Transaction (CIT)	Is any transaction that is not an MIT as defined in section 3.9.1.3, and includes any transaction where the cardholder is available to initiate or authenticate the transaction. Authentication is required for all CITs, unless the transaction qualifies for an exemption or is otherwise out of scope of PSD2
<b>D</b>	
Delegated Authentication	Issuers can delegate authentication to an Acquirer and in turn their qualified Delegates or directly to a token requestor delegate. 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.

Term	Description
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
<b>E</b>	
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"> <li>• Low value exemption</li> <li>• Recurring payment exemption</li> <li>• Trusted beneficiaries exemption</li> <li>• Secure corporate payments exemption</li> <li>• Transaction Risk Analysis (TRA)</li> </ul>
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 2.
<b>L</b>	
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.

Term	Description
<b>M</b>	
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. For a full definition please refer to section 3.9.1.3
<b>O</b>	
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.
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.
<b>P</b>	
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

Term	Description
	European Economic Area (EEA). This requirement is effective as of 14 September 2019 <sup>101</sup> .
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).
<b>R</b>	
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)	<p>An RTS is a standard that supplements an EU directive. An RTS is developed for the European Commission, in the case of PSD2 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>
<b>S</b>	

<sup>101</sup> 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
SCA decline code	A decline code (Response code 1A) used by an Issuer to request that a transaction sent to Authorization without SCA needs to be resubmitted with SCA. This process is also sometimes referred to as a “soft decline”.
Soft decline	The process by which an Issuer requests that a Merchant resubmits for authentication a transaction that has been sent directly to authorization without SCA or with an incorrect out of scope or exemption indicator.
Stand in Processing (STIP)	The component that provides Authorization services on behalf of an Issuer when the Positive Cardholder Authorization System is used or when the Issuer, its VisaNet Processor, or a Visa Scheme Processor is unavailable.
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.
<b>T</b>	
Token Requestor	A Token Requestor (TR) is an entity that requests payment tokens for end-users. Some examples of TRs include digital wallet providers, payment enablers and merchants.
Token Service Providers	Token Service Providers (TSPs) are approved third party partners - connected to VTS and other networks - who help token requestors enable tokenized payments. There are two TSP types: (i) an Issuer TSP (I-TSP) provides solutions for financial institutions in participating token requestors payment services; (ii) a Token Requestor TSP (TR-TSP) allows token requestors to develop consumer digital payment solutions powered by VTS.

Term	Description
Tokenization	Tokenization is the process of replacing the traditional payment card account number with a unique digital token in online and mobile transactions
Transaction Identifier or TRAN ID	The unique identifier assigned to a transaction. This is used to link an out of scope MIT transaction to an original authenticated CIT used to set up the MIT agreement
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"
<b>V</b>	
Visa Attempts Service / Visa Attempts Server	A Visa service that responds to authentication request messages on behalf of the Issuer when either the Issuer does not participate in Visa's 3-D Secure 2.0 Program or the Issuer participates but their ACS is unavailable. The Visa Attempts Server provides proof, in the form of a CAVV, in the authentication response that the merchant attempted to obtain authentication.
Visa Directory Server (DS)	A server hardware/software entity that is operated by Visa, whose primary function is to route authentication requests from merchants to specific ACSs and to return the results of authentication.



Term	Description
Visa Secure	Visa's consumer brand name for EMV 3DS
Visa Token Service (VTS)	The Visa Token Service is a security technology from Visa which replaces sensitive account information, such as the 16-digit primary account number, with a unique digital identifier called a token. The Visa Token Service provides a complete integrated set of tokenization tools for merchants, Issuers, Acquirers and processors.
V.I.P.	The processing component of the VisaNet Integrated Payment System comprised of BASE I and the Single Message System used for single message Authorization in connection with financial Transaction processing.
VMID	Visa Merchant Identifier (VMID). A VMID is a unique 8-digit assigned by Visa to identify each merchant brand business entity, i.e., merchant DBA or Doing-Business-As.

# A Appendices

---

## A.1 Appendix 1 The Stored Credential Framework

A stored credential is 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.

In order to use stored credentials, merchants and their third party agents, payment facilitators, or staged digital wallet operators that offer cardholders the opportunity to store their credentials on file must:

- Obtain cardholder consent through SCA for initial storage of credentials
- Utilize appropriate data values to inform the Issuer of consent and identify initial storage and usage of stored payment credentials

As part of establishing consent to store payment credentials, an initial CIT must be performed indicating that the credentials are being stored. Future transactions using that credential can then be flagged accordingly.

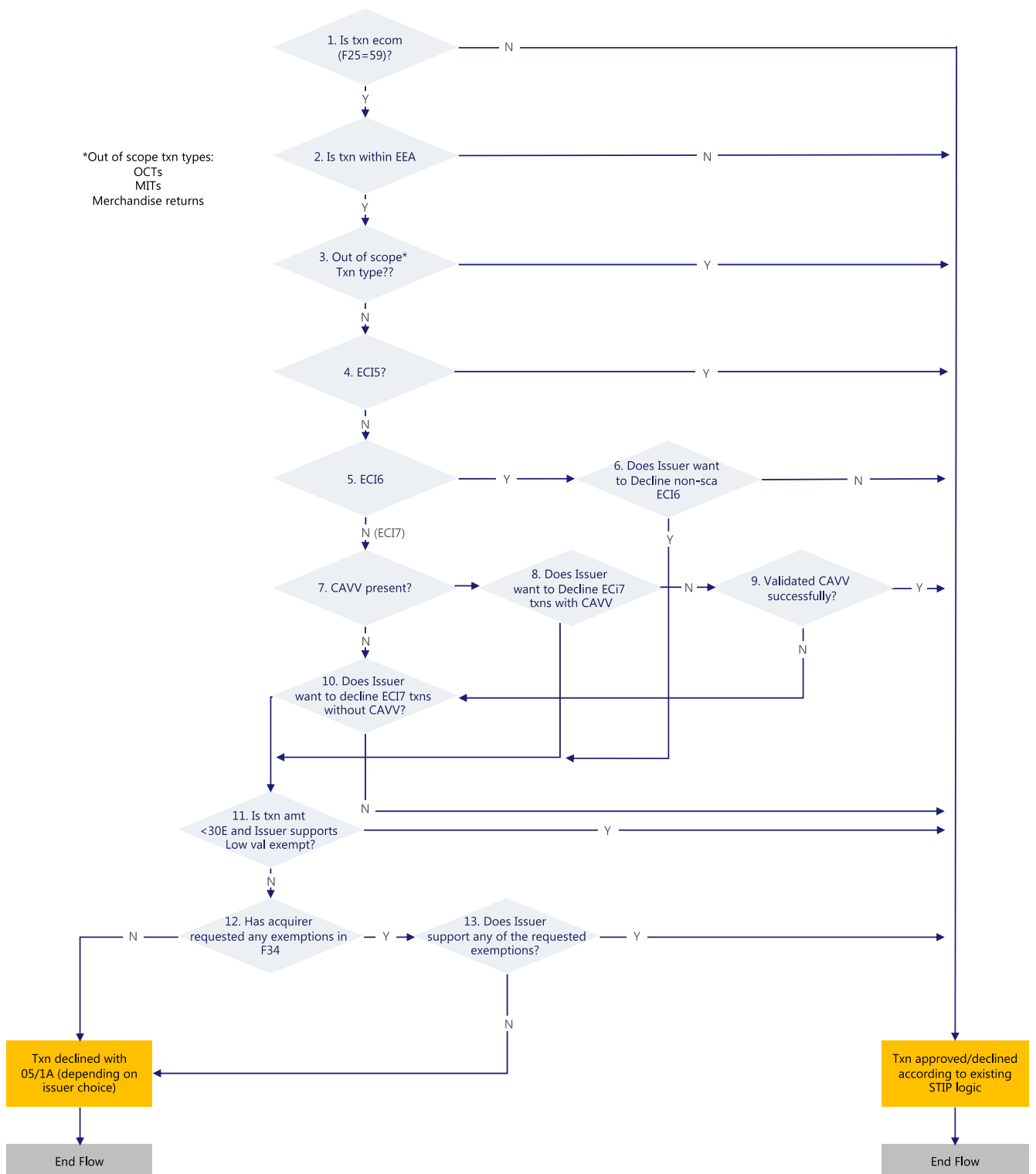
**Table 30: Key data fields for performing CIT transactions with stored credentials**

Transaction Type	Description	POS Entry Mode (F22)	POS environment (F126.13)
CIT	Customer Initiated (CIT) – putting credential on file for first time (e.g. for future use; may be done during a transaction or at account set up via an account verification transaction)	01	C
CIT	Subsequent CIT performed with the Stored Credentials (e.g. shopping online at a merchant or using an app to order a ride)	10	--

Stored payment credentials can be used for CIT or MIT transactions. Details of the data values required for using stored credentials for MIT transactions are included in section 3.9.

## A.2 Appendix 2 STIP SCA Flowchart

Figure 30: STIP SCA flowchart



## A.3 Appendix 3 Merchant Initiated Transactions

Merchants commonly perform MITs without the active participation of the cardholder to:

- Perform a transaction as a follow-up to a cardholder-initiated transaction (CIT)
- Perform a pre-agreed instruction from the cardholder for the provision of goods or services

Examples of MITs include:

- A hotel charge for mini-bar expenses tallied after the guest has checked-out and closed the folio
- A subsequent recurring payment for a magazine subscription

The definition of an MIT and of transactions that do and do not qualify as MITs is given in section 3.9.1.3 and the Visa MIT Framework is summarized in section 3.9. This appendix provides more detail on the types of MIT and the values used to identify them in authorization messages.

The MIT framework covers two types of MITs:

- Industry-Specific Business Practice MITs
- Standing-Instruction MITs

Each transaction type included in the categories is outlined below.

### A.3.1 Industry Specific Business Practice MITs

MITs defined under this category are performed to fulfil a business practice as a follow-up to an original cardholder- merchant interaction that could not be completed with one single transaction. The following transaction types are industry-specific transactions.

- Incremental Authorization Transaction
- Resubmission Transaction
- Delayed Charges Transaction
- Reauthorization Transaction
- No Show Transaction
- Prepayment Transaction

### A.3.2 Incremental Authorization Transaction - Reason Code 3900 in Field 63.3—Message Reason Code

Description	<p>Incremental authorizations can be used to increase the total amount authorized if the authorized amount is insufficient. An incremental authorization request may also be based on a revised estimate of what the cardholder may spend. Incremental authorizations do not replace the original authorization— they are additional to previously authorized amounts. The sum of all linked estimated and incremental authorizations represents the total amount authorized for a given transaction. An incremental authorization must be preceded by an estimated/initial authorization.</p> <p>One or more incremental authorizations can be requested while the transaction has not yet been finalized (submitted for clearing). Incremental authorizations must not be used once the original transaction has been submitted for clearing. Instead, a new authorization must be requested, with the appropriate reason code (e.g., delayed charges, Reauthorization).</p>
Maximum Timeframe between Original Transaction and MIT	<p>Incremental authorizations can be performed during the approval response validity period of the original estimated/initial authorization. For more details, please refer to Visa Rules (ID#: 0029524).</p>
Relevant Merchant Segments	<p>In the EEA and the UK, incremental transactions can be used by e-commerce merchants from any MCC to authorize any additional amount above the initial or estimated authorization request, if the price of merchandise or services, including shipping costs and applicable taxes, has changed.</p> <p>Note that outside of the EEA and the UK, incremental transactions are limited to certain merchant categories. Examples include car rental, lodging, transit, amusement parks, restaurants, and bars. For complete list of all eligible MCCs, refer to the Visa Rules (ID#: 0025596).</p>
Examples	<p>A lodging merchant performs an incremental authorization while adding room service expenses to cardholder’s folio, revising previous estimate of cardholder’s total charges</p>

### A.3.3 Resubmission Transaction—Reason Code 3901 in Field 63.3—Message Reason Code

Description	<p>A merchant performs a Resubmission in cases where it requested an authorization but received a decline due to insufficient funds after it has already delivered the goods or services to the cardholder. Merchants in such scenarios can resubmit the request to recover outstanding debt from cardholders.</p>
Maximum Timeframe between Original Transaction and MIT	<p>Resubmission must be submitted within 14 days from the original transaction. This timeframe limit only applies to token-based resubmissions.</p>

Relevant Merchant Segments	This type of transaction is most prevalent in transit merchant segments, such as commuter transportation including bus lines and passenger railways.
Examples	A transit merchant performs a Resubmission transaction for debt collection after a decline is received due to insufficient funds and the cardholder has already availed the services.

#### A.3.4 Delayed Charges Transaction—Reason Code 3902 in Field 63.3—Message Reason Code

Description	Delayed charge transaction is performed to process a supplemental account charge after original services have been rendered and respective payment has been processed.
Maximum Timeframe between Original Transaction and MIT	Delayed charges must be submitted within 90 days from the date of the rental return, check-out, or disembarkation date, in accordance with the Visa Rules (ID#: 0007398).
Relevant Merchant Segments	Relevant merchant segments are limited to vehicle rental, lodging, cruise lines, and other rentals. For a full list of eligible MCCs for delayed charges, please refer to Visa Rules (ID#: 0007398).
Examples	A lodging merchant performs delayed charge transaction to charge the cardholder for incidental charges such as “mini-bar” charge, after the cardholder has checked out.

#### A.3.5 Reauthorization Transaction—Message Reason Code 3903 in Field 63.3—Message Reason Code

Description	<p>A merchant initiates a Reauthorization when the completion or fulfilment of the original order or service extends beyond the authorization validity limit set by Visa.</p> <p>There are two common Reauthorization scenarios:</p> <ul style="list-style-type: none"> <li>• Split or delayed shipments at e-commerce retailers. A split shipment occurs when not all of the goods ordered are available for shipment at the time of purchase. If the fulfilment of the goods takes place after the authorization validity limit set by Visa, e-commerce merchants perform a separate authorization to ensure that consumer funds are available.</li> <li>• Extended stay hotels, car rentals, and cruise lines. A Reauthorization is used for stays, voyages, and/or rentals that extend beyond the authorization validity period set by Visa</li> </ul>
-------------	--

Maximum Timeframe between Original Transaction and MIT	The following timeframe limits only apply to token-based Reauthorizations. A Reauthorization can be submitted up to 90 days from original purchase except for specific MCCs, which can submit a Reauthorization up to 120 days from the original date of purchase. For the current list of MCCs that can reauthorize for up to 120 days, contact your Visa Representative.
Relevant Merchant Segments	Any merchant category can submit Reauthorization. This type of transaction is most prevalent in e-commerce retail, lodging, car rental, and cruise lines.
Examples	Any merchant category can submit Reauthorization. This type of transaction is most prevalent in e-commerce retail, lodging, car rental, and cruise lines.

### A.3.6 No Show Transaction—Reason Code 3904 in Field 63.3—Message Reason Code

Description	Cardholders can use their Visa cards to make a guaranteed reservation with certain merchant segments. A guaranteed reservation ensures that the reservation will be honored and allows a merchant to perform a no-show transaction to charge the cardholder a penalty according to the merchant's cancellation policy. For merchants that accept token-based payment credentials to guarantee a reservation, it is necessary to perform a CIT (Account Verification Service) at the time of reservation to be able perform a no-show transaction later.
Maximum Timeframe between Original Transaction and MIT	There is no timeframe limit to submit a no-show transaction.
Relevant Merchant Segments	Only certain merchant categories are eligible to guarantee reservations and perform no-show transactions. Qualifying merchant segments include lodging, car rental and other rentals. For complete list of all eligible MCCs that can submit no-show transactions refer to Visa Rules (ID#: 0029266)
Examples	A lodging merchant can perform a no-show transaction to charge a cardholder a penalty for a guaranteed reservation if the cardholder did not cancel the reservation according to the merchant's cancellation policy.

### A.3.7 Standing-Instruction MITs

MITs defined under this category are performed to address pre-agreed standing instructions from the cardholder for the provision of goods or services. The following transaction types are standing-instruction transactions.

- Installment and Prepayment (partial & full) Payment Transaction
- Recurring Payment Transaction

- Unscheduled COF Transaction

### A.3.8 Installment Payment Transaction and Prepayment (partial & full) Transaction —Value “I” in POS Environment Field 126.13

Description	<p>An installment is a transaction in a series of transactions that use a stored credential and that represent a cardholder agreement for the merchant to initiate one or more future transactions over a period for a single purchase of goods or services.</p> <p>A prepayment is one or many payment(s) towards a future purchase of goods/services.</p>
Maximum Timeframe between Original Transaction and MIT	The timeframe is governed by a contract between the consumer and the merchant for that specific installment or prepayment relationship.
Relevant Merchant Segments	<p>Any merchant category can submit installment payment or partial prepayment transactions.</p> <p>Full prepayments are limited to:</p> <ul style="list-style-type: none"> <li>• merchants in the T&amp;E (and related) sectors</li> <li>• Merchants taking an order for custom merchandise or services</li> </ul> <p>Or in a face-to-face environment, where not all goods are able to be collected at the time of purchase and will be shipped at a later date</p>
Examples	<p>A furniture retailer allows a cardholder to pay for goods purchased in installments over a pre-agreed period of time.</p> <p><b>Prepayment (partial):</b> A customer confirms booking a hotel booking, and pays for what is due that day but also agrees to additional prepayment(s) as needed prior to check-in</p> <p><b>Prepayment (full):</b> A customer is pre-ordering a music record that is not scheduled to be released until a later date.</p>

### A.3.9 Recurring Payment Transaction —Value “R” in POS Environment Field 126.13

Description	A transaction in a series of transactions that use a stored credential and that are processed at fixed, regular intervals (not to exceed one year between transactions), representing cardholder agreement for the merchant to initiate future transactions for the purchase of goods or services provided at regular intervals.
Maximum Timeframe between Original Transaction and MIT	The timeframe is governed by a contract between the consumer and the merchant for that specific recurring relationship.
Relevant Merchant Segments	Any merchant category can submit Recurring Payment transactions.
Examples	A magazine publisher charges cardholder for monthly subscription.



**A.3.10      Unscheduled COF Transaction —Value “C” in POS Environment Field 126.13**

Description	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.
Maximum Timeframe between Original Transaction and MIT	The timeframe is generally undetermined, as payment is prompted by a pre-agreed event between the cardholder and merchant in the contract governing their relationship.
Relevant Merchant Segments	Any merchant category can submit unscheduled COF transactions.
Examples	An example of such transaction is an account auto-top up transaction.

## A.4 Appendix 4 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 31 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.

## A.5 Appendix 5 Transaction assessment decision point considerations

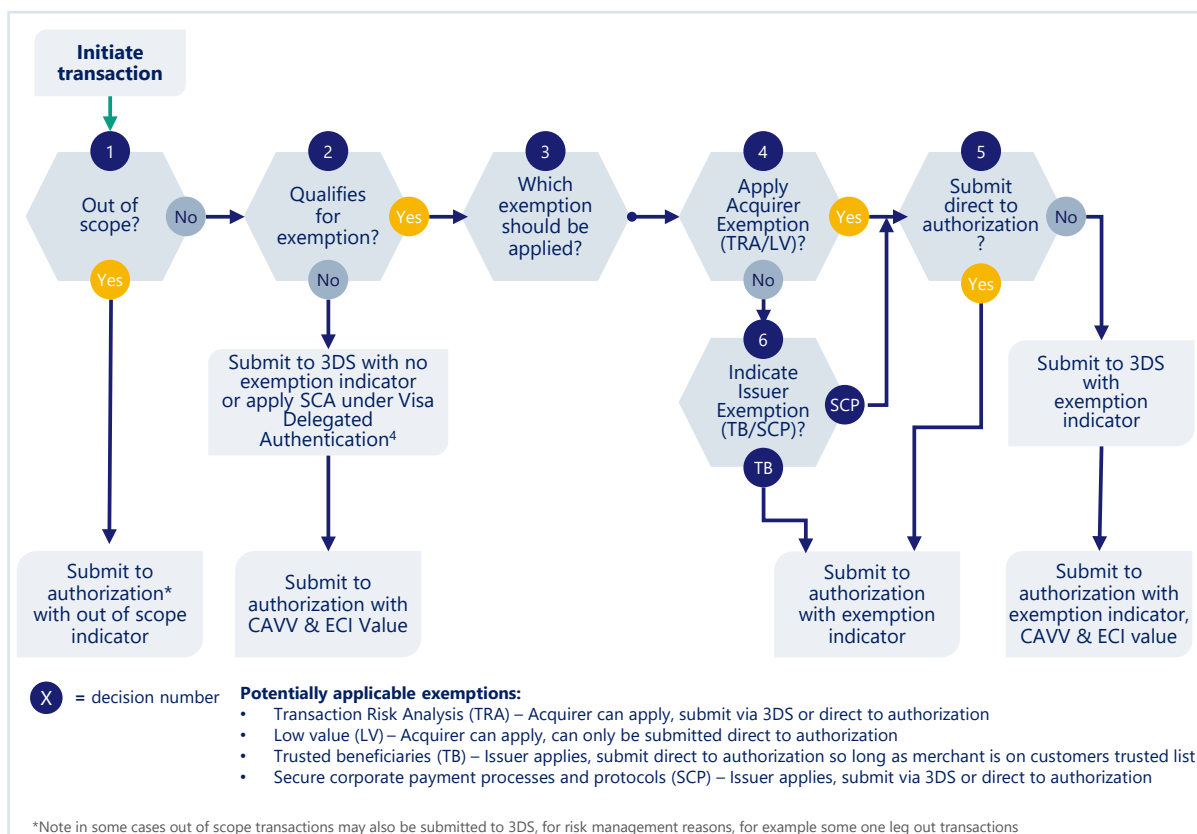
At the individual transaction level, merchants, Acquirers and Issuers move through a sequence of decision points to determine whether:

- The transaction is in or out of scope of PSD2 SCA
- The transaction qualifies for an exemption
- Which qualifying exemption should be applied
- In the case of merchants/Acquirers, how the transaction should be routed, via 3DS or direct to authorization

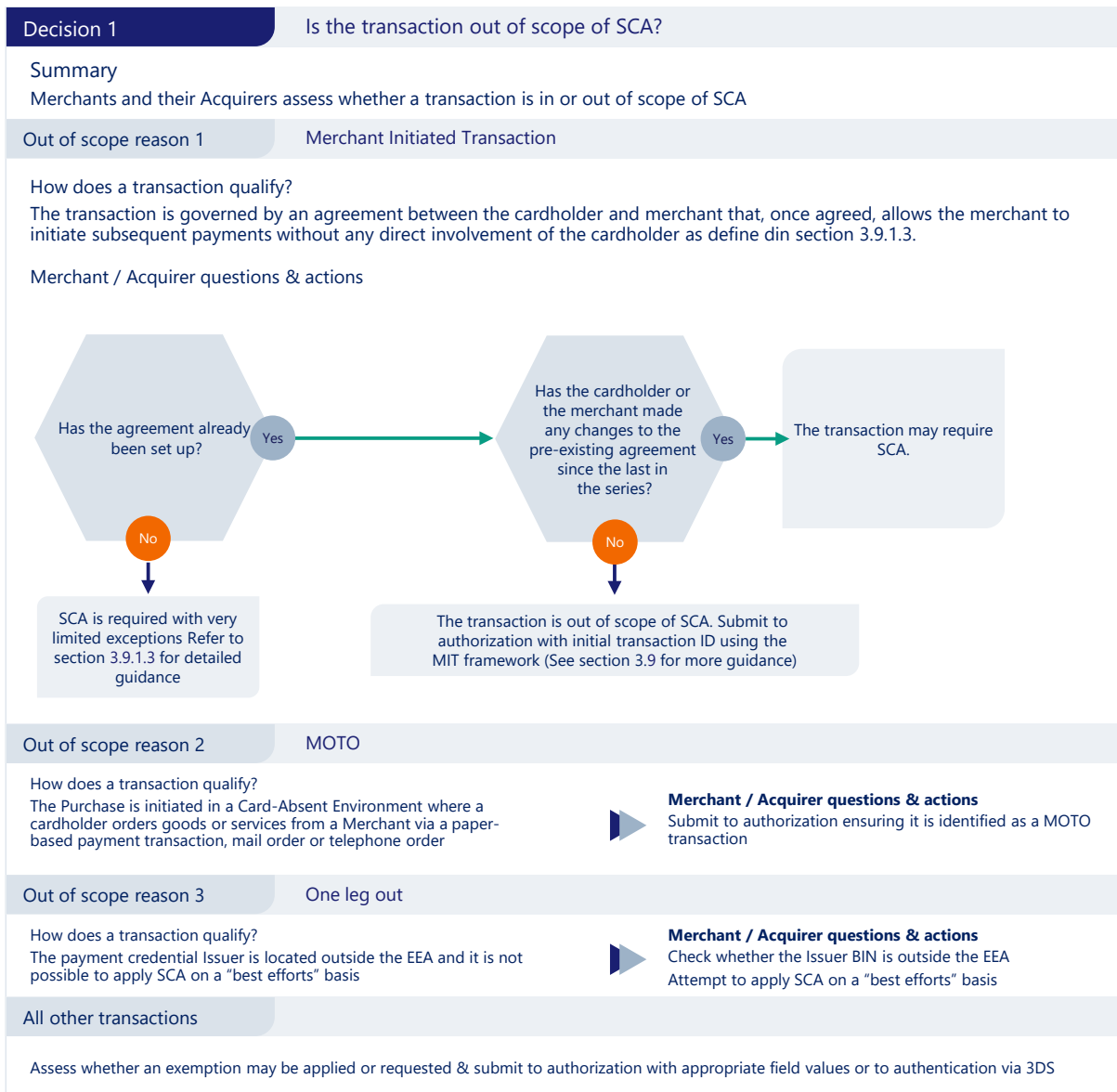
These decision points and the criteria to consider at each decision point are summarized in this appendix

### A.5.1 Merchant/Acquirer decision points

**Figure 31: Key merchant/Acquirer decision points**



**Figure 32 Merchant/Acquirer SCA/exemption simplified process flows and decision points**



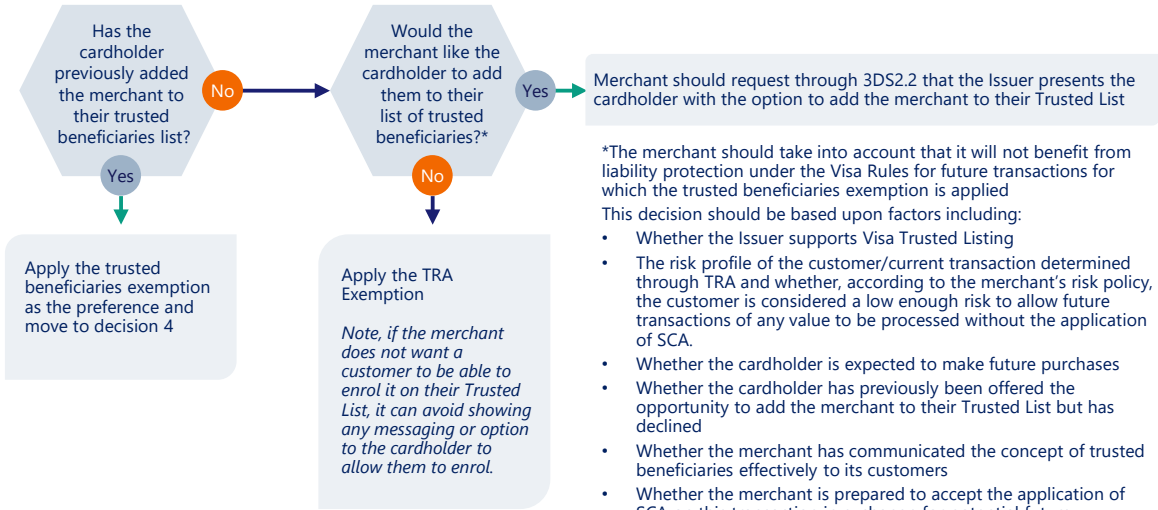
Summary

The TRA or trusted beneficiaries exemption should always take precedence over the low value exemption

Assuming the transaction could qualify for either the trusted beneficiaries or TRA exemption, which exemption should take precedence?

Note: only one exemption should be applied

Decision & Actions



Decision 2

Does the transaction qualify for an exemption?

Summary

Assessment of whether there is an option for the Acquirer to apply or indicate an exemption.

Under the PSD2 regulation, an Acquirer may apply the following exemptions to remote electronic card transactions:

- Transaction Risk Analysis (TRA)
- Low-value transactions
- Recurring transactions

Under the PSD2 regulation an Acquirer may not apply the trusted beneficiaries exemption, however EMV 3DS 2.2.0 and the Visa Trusted Listing Program allow for:

- A cardholder to enrol a merchant in their trusted beneficiaries list while completing an SCA authenticated transaction *and*
- A merchant to be advised 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

Issuers will also apply the secure corporate payments exemption, however under certain circumstances Acquirers may indicate that they consider that a transaction qualifies for the exemption.

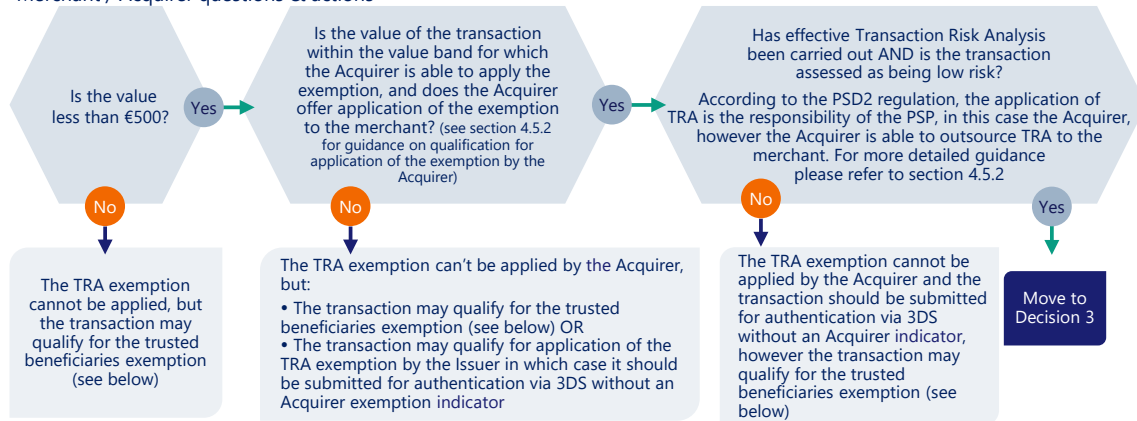
Guidance on assessing the applicability of each transaction type is given below.

Exemption 1 Transaction Risk Analysis (TRA) Exemption

How does a transaction qualify?

- The value of the transaction must be less than €500, *and*:
- The Acquirer's fraud rate must be within the reference fraud rate for the relevant transaction value band, *and*:
- The Acquirer must be prepared to apply the exemption on behalf of the merchant, *and*:
- Transaction Risk Analysis must have been undertaken by the Acquirer or by the merchant on behalf of the Acquirer, and the Transaction Risk Analysis must meet the requirements of the exemption; *and*:
- The transaction must be assessed to be at low risk of fraud

Merchant / Acquirer questions & actions



Exemption 2 Low value exemption

How does a transaction qualify?

- The value of the transaction must be less than €30, *and*:
- The number of consecutive transactions since the last application of SCA must not exceed 5, or the cumulative value of consecutive transactions since the last application of SCA must not exceed €100

*Merchant/Acquirer application not recommended* 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. The Acquirer low value exemption is only supported for transactions submitted direct to authorization

Exemption 3 Recurring Transactions Exemption

How does a transaction qualify?

- The transaction is one of a recurring series of transactions, *and*:
- SCA has been applied when the series was set up, *and*:
- All the payments in the series are of the same amount and made to the same payee.

*Application of this exemption is not supported by Visa* The recurring transactions exemption is not supported within Visa systems. Merchants and Acquirers should treat all recurring transactions as out of scope MITs. For more details please refer to section 3.9

Exemption 4 Trusted Beneficiaries Exemption

How does a transaction qualify?

- Merchant is qualified for application of the trusted beneficiaries exemption, *and*:
- The cardholder has added the merchant to its list of trusted beneficiaries that is held and managed only by the Issuer

Is the merchant enrolled in the Visa Trusted Listing Program? If yes, move to decision 3. If no, Trusted beneficiaries exemption cannot be applied. Submit the transaction for authentication via 3DS without an exemption indicator

Exemption 5 Secure Corporate Payments Exemption

How does a transaction qualify?

- The transaction is undertaken using a commercial virtual card or lodged card, issued to a qualifying "legal person" *or*:
- Subject to the satisfaction of the NCA, a physical commercial card issued to a qualifying is used within a secure corporate payment process or protocol the

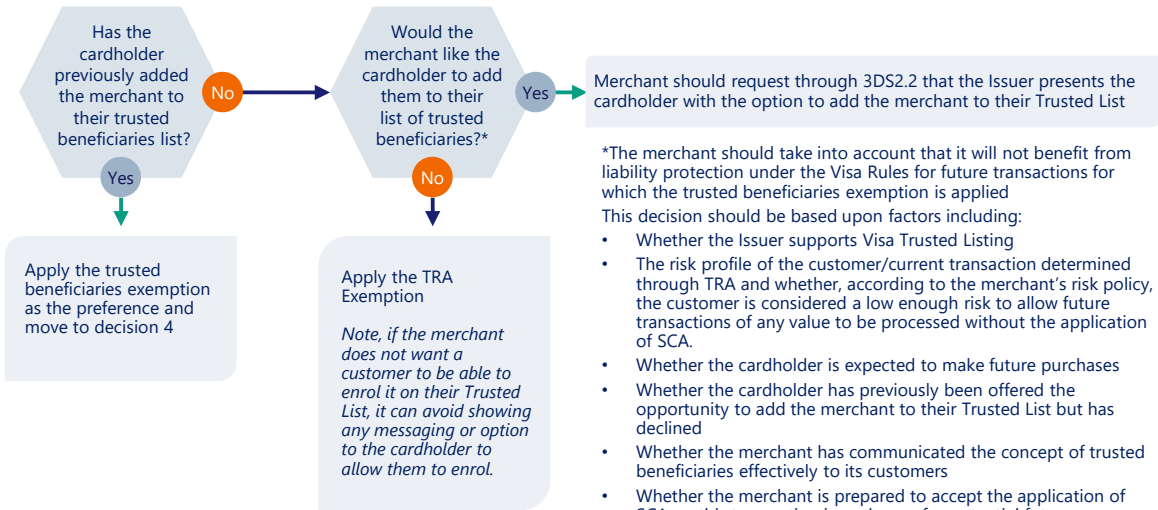
If a virtual card or lodge card is used, this will be recognised and the exemption applied by the Issuer. If a qualifying physical commercial card is used within a qualifying secure payment process or protocol, the Acquirer can request application of the exemption using the secure corporate payments indicator in field 34 and/or 3DS.

Summary

The TRA or trusted beneficiaries exemption should always take precedence over the low value exemption  
 Assuming the transaction could qualify for either the trusted beneficiaries or TRA exemption, which exemption should take precedence?

*Note: only one exemption should be applied*

Decision & Actions



## Decision 4

## Apply an Acquirer TRA or low value Exemption

### Summary

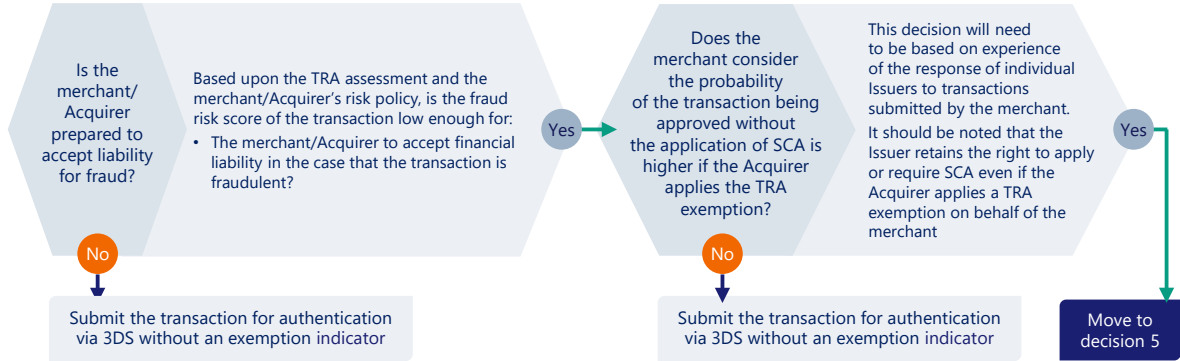
Should an allowable exemption be applied by the Acquirer?

This decision will be based on the merchant/Acquirer's risk strategy and their view on the relative balance between the following factors:

1. Liability protection – which is not available if the exemption is applied by the Acquirer
2. The probability of the Issuer still applying SCA when the Acquirer has applied or requested an exemption

Note: only one exemption may be requested or applied per transaction

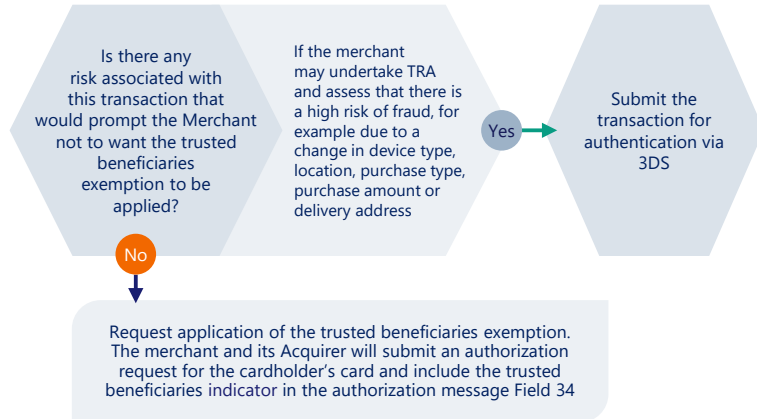
### Transaction Risk Analysis



### Trusted Beneficiaries: Merchant already added to the cardholder's Trusted List

Note, the default position is that if the cardholder is has added the merchant to their Trusted List, the Issuer will apply the trusted beneficiaries exemption unless:

- The Acquirer assesses there is risk associated with the transaction and submits it via 3DS for authentication, or
- The Issuer assesses there is risk associated with the transaction and applies SCA





## Decision 5

### Submit the transaction straight to authorization?

#### Summary

The low value Acquirer exemption can only be applied on transactions submitted straight to authorization

A merchant submitting a transaction with an Acquirer TRA exemption applied has the option to either submit via 3DS or straight to authorization with appropriate indicators set (see section 3.2.2 for details)

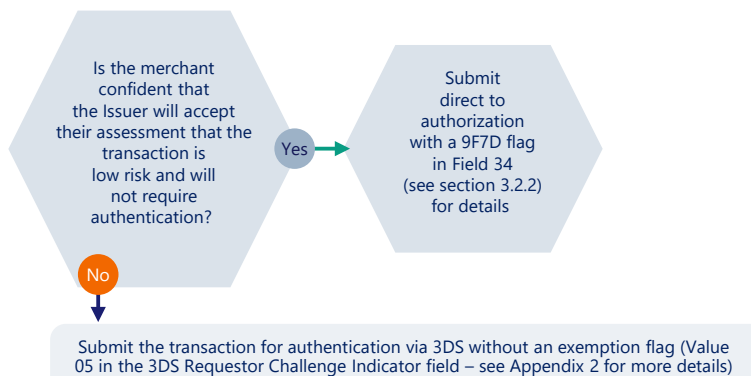
The decision will be based on the merchant's assessment of the balance between the following factors:

- The merchant's own level of confidence in their assessment of the risk of the transaction
- A balanced evaluation of the risk that any challenge may present to the cardholder abandoning the transaction
- The potential benefit of liability protection that comes with a fully authenticated 3DS transaction
- Their confidence that the Issuer will accept their assessment that the transaction is low risk and will not require SCA
- The cost of submission via 3DS vs. direct to authorization

*It should be noted that if a transaction is submitted straight to authorization with an Acquirer TRA exemption flag, the Issuer has the right to request that it is resubmitted for authentication via 3DS potentially adding latency and cost to transaction authentication and authorization process.*

A transaction originating in a qualifying secure corporate environment, and in the view of the NCA qualifies for the secure corporate payments exemption can be submitted via 3DS or straight to authorization with the appropriate indicator.

#### Transaction Risk Analysis



## Decision 6

### Indicate trusted beneficiaries or secure corporate payments exemption?

#### Summary

If the transaction qualifies for the exemption and the merchant/acquirer does not detect a specific risk, the transaction should be submitted with the appropriate exemption indicator

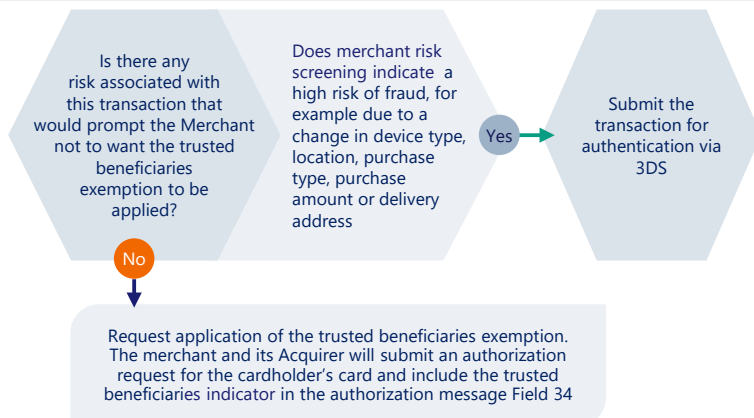
If the transaction originated in a qualifying secure corporate environment, and in the view of the NCA qualifies for the secure corporate payments exemption, and the merchant and their Acquirer are able to support it, the merchant should flag the exemption using the secure corporate exemption indicator in F34 of the authorization request and, if submitting via 3DS, the EMV 3DS SCP extension.

If the transaction qualifies for the trusted beneficiaries exemption see below:

#### Trusted Beneficiaries Exemption

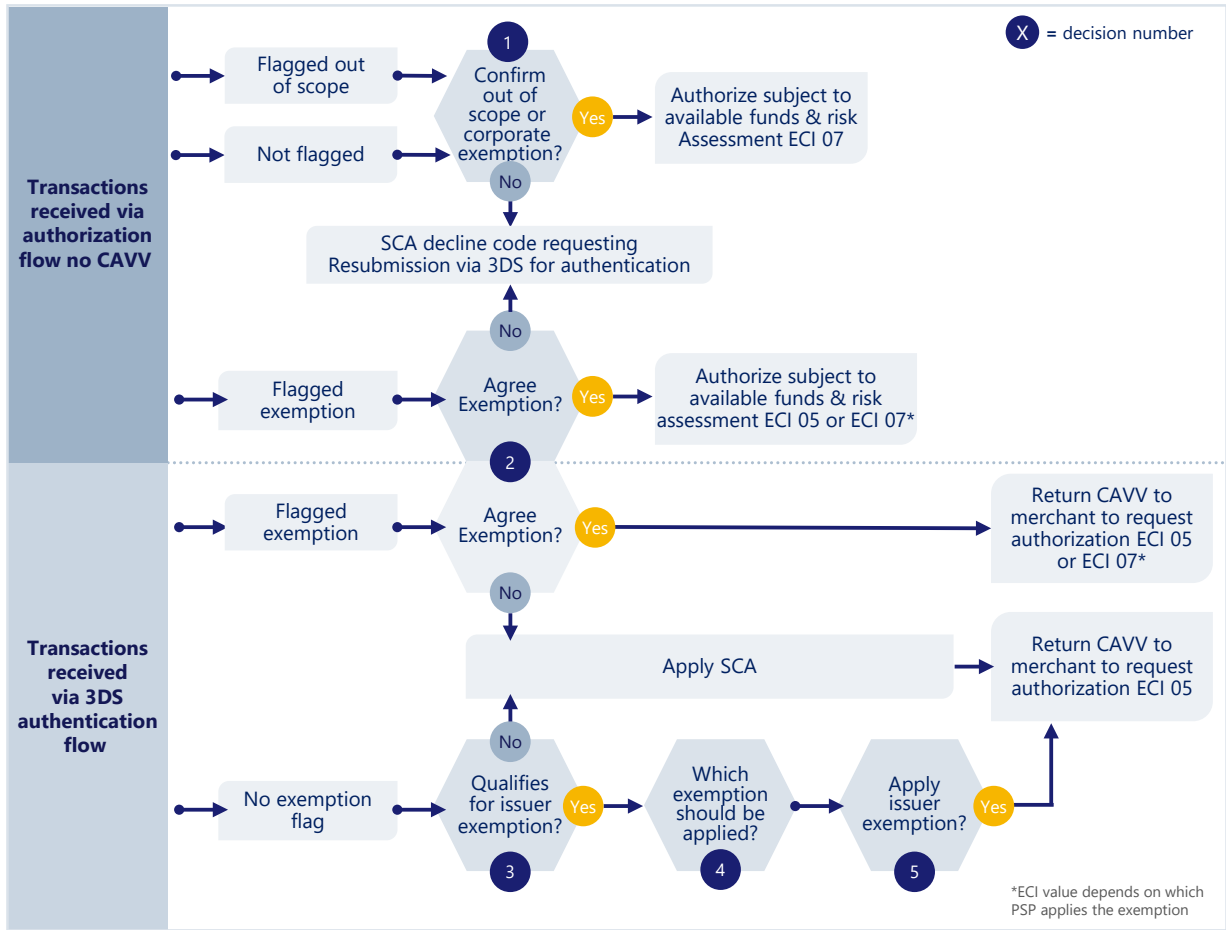
Note, the default position is that if the cardholder is has added the merchant to their Trusted List, the Issuer will apply the trusted beneficiaries exemption unless:

- The Acquirer assesses there is risk associated with the transaction and submits it via 3DS for authentication, or
- The Issuer assesses there is risk associated with the transaction and applies SCA



## A.5.2 Issuer decision points

Figure 33: Key Issuer decision points



**Figure 34: Issuer key decision flow**

Decision 1		Confirm the Transaction is out of scope of or does not otherwise require SCA
<p><b>Summary</b>                      Issuer assess whether a transaction received with an out of scope indicator is out of scope of SCA or otherwise does not require SCA. For more information on identifying out of scope and other transactions not requiring SCA please see section 3.2.9</p>		
Out of scope reason 1		Merchant Initiated Transaction
<p>How does a transaction qualify?                      The transaction is received with an appropriate indicator</p>	▶	<p><b>Issuer actions</b>                      If the correct MIT indicator is present, the transaction is an MIT and SCA is not required (subject to the interpretation of your NCA). You may optionally wish to check the Original Tran ID to ensure it refers to a valid CIT (or in some cases to a valid previous MIT), however be aware that there are valid reasons why the initial CIT may not have been authenticated. In some instances a Visa assigned Tran ID may be used for an interim period of time rather than a valid number. Refer to section 3.9.3 for more information on identification of MITs                      Authorize, subject to normal authorization assessment criteria (availability of funds etc)                      The Issuer must not issue an SCA decline code due to lack of authentication</p>
Out of scope reason 2		MOTO
<p>How does a transaction qualify?                      The transaction is received with an appropriate indicator</p>	▶	<p><b>Issuer actions</b>                      Authorize, subject to normal authorization assessment criteria.                      Do not decline or issue an SCA decline code due to lack of authentication</p>
Out of scope reason 3		Anonymous payment
<p>How does a transaction qualify?                      The payment credential is not directly linked to an individual consumer (for example an anonymous prepaid gift card)</p>	▶	<p><b>Issuer actions</b>                      When you receive an authorization for a card from an anonymous card BIN, authorize, subject to normal authorization assessment criteria (availability of funds etc).                      Do not decline or issue an SCA decline due to lack of authentication</p>
Out of scope reason 4		One-Leg-Out
<p>How does a transaction qualify?                      The Acquirer is outside the EEA.</p>	▶	<p><b>Issuer actions</b>                      Authorize, subject to normal authorization assessment criteria (availability of funds etc).                      Do not decline or issue an SCA decline code -due to lack of authentication                      Issuers should continue to use their ACS to authenticate whenever the merchant has initiated a 3DS authentication request (subject to applicable exemptions, or application of SCA on a best efforts basis) or authorize accordingly</p>
Other Transactions not requiring SCA		
<p>How does a transaction qualify?                      OCTs, refunds &amp; some zero value authorization/verification requests</p>	▶	<p><b>Issuer actions</b>                      Check for indicators described in section 3.2.9 and account verification transaction scenarios described in 4.7.3.2.                      Do not decline or issue an SCA decline code due to lack of authentication</p>
Unflagged Transactions		
<p>Why is the transaction unflagged?                      Some transactions can be legitimately be submitted direct to authorization by a merchant without an out of scope exemption flag being applied. These include corporate payments using commercial virtual or lodged cards and transactions using anonymous cards.</p>	▶	<p><b>Issuer actions</b>                      Check the BIN to establish whether the card is legitimately out of scope (an anonymous card) or whether an Issuer applied exemption (The secure corporate payments and processes exemption) applies.                      Do not decline or issue an SCA decline code due to lack of authentication</p>

Decision 2

Does the Issuer agree with the Acquirer applied or indicated exemption?

Summary

Under the PSD2 regulation, an Acquirer may apply the following exemptions to remote electronic card transactions:

- Transaction Risk Analysis (TRA)
- Low-value transactions
- Recurring transactions

Under the PSD2 regulation an Acquirer may not apply the trusted beneficiaries exemption, however 3DS 2.2 and the Visa Trusted Listing Program allow for:

- A cardholder to add a merchant in their Trusted List while completing an SCA authenticated transaction and
- A merchant to be advised as to whether it is on a cardholder’s Trusted List and, if so, to indicate to the Issuer that it would like the exemption to be applied

Visa recommends that Acquirers should not apply the low value transaction exemption as they do not have visibility of the velocity limits, or the recurring transactions exemption as recurring card transactions should be treated as MITs.

Under certain circumstances, specifically when a physical commercial card issued to an individual is used within an approved secure environment, Acquirers may indicate that they consider that a transaction qualifies for the secure corporate payments exemption.

The Issuer has the right to apply SCA if it assesses a transaction to be high risk even if the Acquirer has applied or requested an exemption.

Issuers may receive transactions flagged with an Acquirer exemption through either the authorization or authentication flow. The Acquirer assumes liability unless the Issuer overrides the application of the exemption and applies SCA.

Exemption 1 Transaction Risk Analysis (TRA) exemption

How does a transaction qualify?

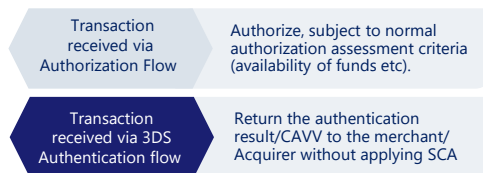
- The value of the transaction must be less than €500, and;
- The Acquirer’s fraud rate must be within the reference fraud rate for the relevant transaction value band, and;
- The Acquirer must be prepared to apply the exemption on behalf of the merchant, and;
- Transaction Risk Analysis must have been undertaken by the Acquirer or by the merchant on behalf of the Acquirer; and;
- The transaction must be assessed to be at low risk of fraud; and;
- The merchant/Acquirer submits the transaction straight to authorization or via with an appropriate exemption indicator

Issuer options and actions:

a) Allow the exemption

The Issuer may choose to do this on the basis that:

- RBA has been applied and the Issuer considers the transaction to be low risk
- The Acquirer is within its TRA permitted fraud rate
- The merchant/Acquirer will assume liability for fraud



b) Require the application of SCA

The Issuer may choose to do this on the basis that:

- RBA has been applied and the Issuer considers the transaction to be high risk
- The Issuer has received insufficient transaction data to confidently assess the risk of the transaction



Exemption 2 Trusted beneficiaries exemption

How does a transaction qualify?

- The Merchant participates in the Visa Trusted Listing Program
- The cardholder has added the merchant to its Trusted List that is held and managed only by the Issuer

Issuer options and actions

The Issuer may accept the exemption if:

- The Issuer considers the transaction to be low risk
- There is no suspicious activity on this card



Exemption 3 Secure corporate payments exemption

How does a transaction qualify?

- A physical commercial card issued to a qualifying “legal person” is used within a secure corporate payment process or protocol to the satisfaction of the NCA

Issuer options and actions

Subject to the Issuer’s risk policy on application of the secure corporate payments exemption, the Issuer should either:

- apply the exemption if it considers the transaction was initiated in a legitimate secure corporate environment
- Decline the transaction with an SCA decline code, if it considers that the transaction was not initiated in a secure corporate environment.

## Decision 3

## Does the transaction qualify for an Issuer exemption?

### Summary

Assessment of whether there is an option for the Issuer to apply an exemption

Where the Issuer has received a transaction via 3DS without an Acquirer exemption indicator, the Issuer should assess whether the transaction qualifies for an exemption and should seek to apply the most appropriate qualifying exemption to minimise the impact of authentication on the customer experience.

Under the PSD2 regulation, an Issuer may apply the following exemptions to remote electronic card transactions:

Transaction Risk Analysis (TRA)

Low-value transactions

Trusted beneficiaries

Secure corporate payments

Note: While the PSD2 regulation allows for the Issuer to apply this exemption for card transactions, Visa does not support the recurring transactions exemption within its systems. Recurring card transactions should be treated as MITs and out of scope

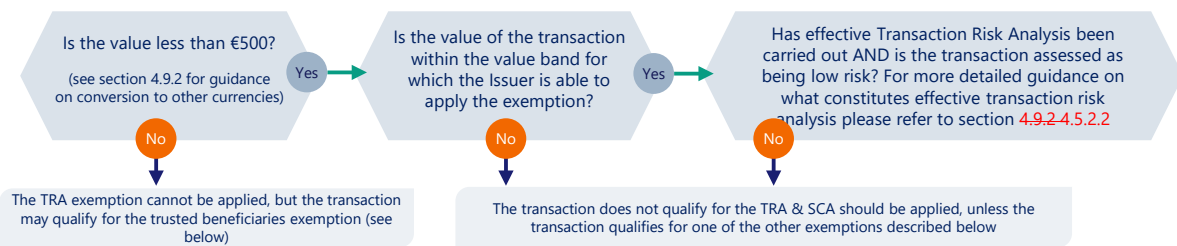
### Exemption 1

#### Transaction Risk Analysis (TRA)

How does a transaction qualify?

- The value of the transaction must be less than €500, and:
- The Issuer's fraud rate must be within the reference fraud rate for the relevant transaction value band, and:
- Transaction Risk Analysis must have been undertaken by the Issuer, and:
- The transaction must be assessed to be at low risk of fraud

Issuer questions & actions



### Exemption 2

#### Low Value

How does a transaction qualify?

- The value of the transaction must be less than €30, and greater than €0 and:
- The number of number of consecutive transactions since the last application of SCA must not exceed 5, or the cumulative value of consecutive transactions since the last application of SCA must not exceed €100

Issuer options and actions

- So long as the Issuer determines that the qualifying criteria apply, the Issuer may apply the low value transaction exemption.
- The Issuer should still however apply RBA as required by the PSD2 regulation and should apply SCA if the transaction is perceived to be at risk of fraud.
- The Issuer should consider that it will be liable for any fraud and will also be have to take account of the value of that fraud in its fraud count in determining whether it qualifies for application of the TRA exemption
- The low value exemption should not be applied to account verification transactions and velocity counters should not be incremented for these transactions as the application of SCA is not required.
- Issuers applying the exemption to transactions submitted via 3DS, should ensure their ACS is linked in real time to the velocity checking in the Issuer's authorization system to prevent SCA decline codes being issued for transactions that have breached counts when submitted to authorization. See section 4.5.1 for more information

### Exemption 3

#### Trusted beneficiaries

How does a transaction qualify?

- The Merchant participates in the Visa Trusted Listing Program
- The cardholder has added the merchant to its Trusted List that is held and managed only by the Issuer

Issuer options and actions

So long as the Issuer determines that the qualifying criteria **apply**, and the transaction is not assessed to be **at risk of fraud**, the Issuer may apply the trusted beneficiaries exemption.

### Exemption 4

#### Secure corporate payments

How does a transaction qualify?

- The transaction is made through a secure dedicated corporate process or protocol and the NCA is satisfied the processes or protocols used guarantee at least equivalent levels of security to those provided for by PSD2, the payer is not a consumer and is considered a "legal person" in the view of the NCA, AND
- The transaction may have been flagged by the acquirer using the SCP indicator
- The Issuer may have identified that the transaction is made using a qualifying virtual card or lodged card/Central Travel Account

Issuer options and actions

So long as the Issuer determines that the qualifying criteria apply, and the transaction is not assessed to be at risk of fraud, the Issuer may apply the secure corporate payments exemption.

#### Decision 4

#### Which applicable exemption should take priority?

##### Summary

Assuming the transaction could qualify for either the TRA, low value, trusted beneficiaries or secure corporate payments exemption, which should take precedence?

This decision will depend on the transaction type.

- For standard consumer transactions, where the merchant is not on the customers Trusted List, the TRA exemption should be applied first so long as the transaction qualifies.
- If the transaction does not qualify for the TRA exemption but does qualify for the low value exemption, the low value exemption should be applied, subject to the considerations outlined in Decision 3.
- The trusted beneficiaries exemption should be applied to transactions where the merchant is on a customers' Trusted List, so long as RBA analysis does not identify the transaction as high risk
- The secure corporate payments exemption should be applied to flagged qualifying transactions and transactions using Virtual Cards and Lodged cards issued to qualifying customers, so long as the RBA analysis does not identify the transaction as high risk

#### Decision 5

#### Apply an Issuer Exemption?

##### Summary

**Summary:** Should an allowable exemption be applied by the issuer?

**So long as a transaction qualifies for an exemption and the issuer does not assess that there is an unacceptable risk of fraud, the issuer should apply the exemption in order to minimise cardholder friction and abandonment.**

**Note, only one exemption may be applied per transaction**