



# PSD2 SCA for Remote Electronic Transactions Implementation Guide

November 2019

# Contents

---

<b>Important Information .....</b>	<b>5</b>
<b>Using this document.....</b>	<b>6</b>
<b>What has changed in Version 2.0 .....</b>	<b>9</b>
<b>1. Introduction: Visa's guiding principles for PSD2 .....</b>	<b>21</b>
1.1 Introduction.....	21
1.2 Visa's guiding principles.....	21
<b>2. The requirements of PSD2 Strong Customer Authentication and Visa's interpretation .....</b>	<b>22</b>
2.1 The application of SCA and use of factors .....	23
2.2 Exemptions .....	24
2.3 Out of scope transactions.....	25
2.4 Dynamic linking .....	26
2.5 Visa PSD2 Solutions and GDPR.....	26
<b>3. Visa's PSD2 solutions.....</b>	<b>27</b>
3.1 Solution summary .....	27
3.2 Authorization options.....	29
3.3 3-D Secure .....	42
3.4 Visa's PSD2 solutions using Visa Token Service (VTS) .....	60
3.5 Visa Rules & policies for PSD2 & 3DS.....	62
3.6 Visa Trusted Listing .....	67
3.7 Visa Transaction Advisor .....	69
3.8 Visa Delegated Authentication .....	71
3.9 Visa Merchant Purchase Inquiry (VMPI) .....	72
3.10 The Visa MIT Framework.....	74
3.11 Visa Biometrics.....	84
3.12 Visa Consumer Authentication Service.....	85
<b>4. Optimising the payment experience under PSD2 .....</b>	<b>86</b>
4.1 Introduction.....	86
4.2 Key principles.....	87
4.3 Step by step guide to managing the authentication flow.....	102
4.4 Liability for fraud-related chargeback.....	114
4.5 Additional guidance on application of the exemptions.....	116

4.6	Additional Guidelines for Issuers .....	124
4.7	3DS and authorization fall-back options .....	135
4.8	Visa Direct and SCA under PSD2.....	139
4.9	Visa Checkout and Visa Secure Remote Commerce.....	141
4.10	Visa Secure Authentication Technology and non-Visa Transactions .....	141
<b>5.</b>	<b>Payment use cases and sector specific guidance for merchants and PSPs.....</b>	<b>142</b>
5.1	Inclusion of authentication-related data.....	142
5.2	One-time purchase.....	146
5.3	Delayed Shipment.....	147
5.4	Split Shipment.....	150
5.5	Open orders - Unknown final amount.....	153
5.6	Aggregated payments.....	158
5.7	Real-time service via mobile app with payment after service /completion.....	161
5.8	Omni-channel purchases .....	166
5.9	Resubmission of declined authorization on contactless transit transactions .....	167
5.10	Accessing stored credentials using QR codes.....	168
5.11	Establishing a new agreement for future MITs.....	169
5.12	Changing agreement payment terms .....	172
5.13	Executing payments based on established agreements.....	173
5.14	Visa Direct payment.....	180
5.15	B2B payments.....	181
5.16	Multi-party commerce .....	185
5.17	Industry Specific Best Practice.....	187
5.18	Non-financial scenarios .....	188
5.19	Provisioning Network Tokens.....	190
5.20	Mass tokenising existing credential on file .....	190
<b>6.</b>	<b>Planning for PSD2 – what you need to do .....</b>	<b>191</b>
6.1	Issuer planning checklist .....	191
6.2	Acquirer planning checklist.....	196
6.3	Merchant planning checklist.....	198
<b>7.</b>	<b>Bibliography .....</b>	<b>200</b>
<b>A</b>	<b>Appendices .....</b>	<b>210</b>
A.1	Appendix 1 EMV 3DS Data Elements .....	210
A.2	Appendix 2 Authentication Message Fields.....	215
A.3	Appendix 3 Considerations for Implementing OOB Biometrics on EMV 3DS 2.1.0 and 2.2.0 .....	218

A.3.1 Introduction.....	218
A.3.2 Recommendations for optimizing consumer experience applicable to desktop and mobile browser and app flows.....	219
A.3.3 Additional recommendations relevant to desktop browser purchases.....	221
A.3.4 Additional recommendations relevant to mobile browser purchases.....	221
A.3.5 Additional recommendations relevant to mobile app purchases.....	222
A.4 Appendix 4 The Stored Credential Framework.....	224
A.5 Appendix 5 STIP SCA Flowchart .....	225
A.6 Appendix 6 Merchant Initiated Transactions.....	226
A.6.1 Industry Specific Business Practice MITs .....	226
A.6.2 Incremental Authorization Transaction - Reason Code 3900 in Field 63.3—Message Reason Code .....	227
A.6.3 Resubmission Transaction—Reason Code 3901 in Field 63.3—Message Reason Code .....	227
A.6.4 Delayed Charges Transaction—Reason Code 3902 in Field 63.3—Message Reason Code .....	228
A.6.5 Reauthorization Transaction—Message Reason Code 3903 in Field 63.3—Message Reason Code .....	228
A.6.6 No Show Transaction—Reason Code 3904 in Field 63.3—Message Reason Code .....	229
A.6.7 Standing-Instruction MITs .....	229
A.6.8 Installment Payment Transaction and Prepayment (partial & full) Transaction — Value "I" in POS Environment Field 126.13.....	230
A.6.9 Recurring Payment Transaction —Value "R" in POS Environment Field 126.13 ....	230
A.6.10 Unscheduled COF Transaction —Value "C" in POS Environment Field 126.13	231
A.7 Appendix 7 EEA Countries in scope of PSD2 SCA .....	232

# 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 of the specification is referred to as EMV 3DS 2.1.0 and version 2.2 is referred to as EMV 3DS 2.2.0.

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 compliance 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 7.

This guide covers remote electronic payments (e-commerce and m-commerce).

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 compliance
2	The requirements of PSD2 Strong Customer Authentication and Visa’s interpretation	Summarizing Visa’s interpretation of the PSD2 SCA requirements, including implementation and enforcement approaches following the publishing of the EBA opinions in June 2019 and October 2019, the application of SCA and the exemptions allowed
3	Visa’s PSD2 SCA Solutions	Providing the essential information needed to interpret Sections 4 and 5 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>

		<ul style="list-style-type: none"> <li>Considerations to take into account when deciding how to handle transactions</li> </ul> <p>Guidance on managing of out of scope transactions and individual exemptions</p>
5	Payment use cases and sector specific guidance for merchants and PSPs	<p>Describing the recommended authentication and authorization flows for key common and complex payment use cases</p> <p>The section provides merchants with additional guidance on the application of SCA to specific payment scenarios, such as split and delayed shipments and subscriptions</p>
6	Planning for PSD2 – what you need to do	<p>Providing checklists for merchants, Acquirers and Issuers, highlighting the actions they need to take to plan and execute the implementation of PSD2 SCA</p>
7	Bibliography	A list of key additional reference documents
8	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 specs 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 processing of eCommerce 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 [PSD2questions@visa.com](mailto:PSD2questions@visa.com).



# What has changed in Version 2.0

The following table summarizes the main changes to the content between version 1.1 and 2.0 of this guide. Please note:

- This version of the guide includes a substantial number of changes over the previously published V1.1
- The aim of the below table is to direct readers to new or substantially changed content. The table does not include minor wording changes that do not impact on the meaning of the guidance.
- Many of the changes summarized here are complex and detailed and readers should review carefully each revised section to ensure that they understand the guidance
- The section numbers listed below refer to the sections in this version 2.0 of the guide.

Section	Topic	Description of Change
Using this document	Card present and contactless payments	Statement added that SCA applies to card present and contactless payments and referencing the Guide "Visa Contactless and Card Present PSD2 SCA: A Reference Guide to Implementation".
2	EBA Opinion covering enforcement timescales	Additional explanation added summarizing the EBA Opinion papers published 21 June 2019 and 16 October 2019 recognizing the need for delay in enforcement and Visa's proposed approach to SCA roll outs, roadmap and adoption of EMV 3DS 2.2.0.
2.1	Use of factors	Summary of Visa's proposed SCA Authentication Factor Strategy added following the EBA Opinion that neither card details nor OTPs can be used as a knowledge element.
2.2.5	Recurring transactions	New paragraph added confirming that recurring card transactions should be treated as out of scope MITs.

2.5	GDPR	Addition of a statement summarizing the position of Visa's PSD2 solutions with respect to GDPR.
3.1	Authentication and Authorization	Addition of definitions of authentication and authorization and a summary introduction to the authentication and authorization process flows to provide context to the subsequent more detailed descriptions.
3.2.2	Authorization fields and messages (Table 4)	Update to details of Field 34 tags used to indicate or request application of exemptions or indicate an MIT is out of scope.
3.2.3	VisaNet Field 34 & Response Code 1A in Field 39	Update to details of Field 34 tags used to indicate or request application of exemptions or indicate an MIT is out of scope.
3.2.3.1	Field 34 and Response code 1A Impact for Acquirers	Clarification of the impact if the Acquirer's parameter is activated in VisaNet to receive response code 1A and of certification requirement.
3.2.4	MIT out of scope indicator	New section added covering MIT out of scope indicator for Issuers in Field 34.
3.2.7	Identification of out of scope transactions	Addition of guidance stating how out of scope transactions and other transactions that do not require SCA by the cardholder (Original Credit Transactions and refunds) should be indicated and recognized.
3.3	Use cases for 3-D secure	Addition of guidance confirming that 3-D Secure may be used both for authenticating payment transactions and confirming cardholder consent to setting up a mandate for a series of MITs.
3.3	Visa Secure brand	Addition of a statement on the use of "Visa Secure" for consumer branding of Visa 3-D Secure solutions.
3.3.2	EMV 3DS implementation requirements & timescales	Addition of information on Visa rule changes and requirements on Issuers to implement EMV 3DS 2.1.0 March 2020 and EMV 3DS 2.2.0 by September 2020. Section covers updated timing of EMV 3DS Implementation date and liability shift.

3.3.3	The Visa roadmap for PSD2 SCA & 3DS implementation	Addition of an updated roadmap showing key milestones for 3DS implementation.
3.3.4	3DS version feature comparison	Addition of tables comparing the feature support of 3DS 1.0, EMV 3DS 2.1.0 and EMV 3DS 2.2.0 and describing key features.  Addition of more information on 3RI including the transaction flow.
3.3.4.1	3RI Payments	Addition of a 3RI flow diagram.
3.3.7	Roles of the Issuer and the Issuer's ACS in the application of 3DS	Addition of summary statement on the roles of the Issuer and the Issuer's ACS in the application of 3-D Secure.
3.3.14	The co-existence of 3DS 1.0 and EMV 3DS	Guidance updated to make the process of identifying Issuer 3DS version support clearer and to reinforce the message to merchants to submit the correct version.
3.4	Visa's PSD2 solutions using Visa Token Service (VTS)	Addition of a summary of VTS and the Visa Token Framework and an introduction to the way they are used within Visa's PSD2 solution portfolio.
3.5	Visa Rules & policies for PSD2 & 3DS	Updated summary of relevant Visa Rules, policies and addition of a reference to the supporting guide detailing the rules.
3.6	Visa Trusted Listing	Updated section on Visa Trusted Listing with additional information and reference to Visa Trusted Listing Implementation Guide.
3.7	Visa Transaction Advisor	Updated section on Visa Transaction Advisor with additional information and reference to Visa Transaction Advisor Implementation Guide.
3.8	Visa Delegated Authentication	Updated section on Visa Delegated Authentication with additional information and reference to Visa Delegated Authentication Implementation Guide.
3.9	Visa Merchant Purchase Inquiry	Addition of new section describing Visa Merchant Purchase Inquiry.

3.10	The Visa MIT Framework	Section substantially updated to include more information including a summary of key data values and fields used with MIT transactions.
3.11	Visa Biometrics	Additional information added on Visa Biometrics.
3.12	Visa Consumer Authentication Service (VCAS)	Minor wording change to clarify that VCAS uses Risk Based Authentication capabilities and reference to link for additional information added.
4.1	Merchants and Acquirers requesting exemptions	Addition of guidance that merchants and Acquirers should only request one exemption and set one exemption indicator.
4.2.1	The difference between Authentication and Authorization	Correction of definition of Authentication.
4.2.2	Dynamic Linking	Addition of guidance describing how the dynamic linking requirement is met using the CAVV or TAVV.
4.2.4.1	Out of scope transactions	Removal of previously included summary table on out of scope transactions and inclusion of reference to new section 3.2.7 on flagging and identifying out of scope transactions.
4.2.4.2.1	Summary of Common CIT & MIT payment use cases- Table 25	Minor changes to table 17 to reflect European Commission and EBA confirmation that MITs are out of scope.
4.2.4.2.1	Summary of Common CIT & MIT payment use cases- Table 25	MIT third use case wording updated to clarify the linking of the MIT to the original CIT.
4.2.4.3	Visa authentication, authorization and clearing principles for implementing SCA – Table 27	Wording changes to principles 3, 7, 8, 9, 12, 13, 15, 16, 17 to clarify.
4.2.5	Application of exemptions	Note added to table confirming that Visa does not provide an indicator for the recurring transaction exemption as recurring card payments should be processed as MITs.
4.2.6	Options for merchants and Acquirers regarding the application	Addition of diagram to clarify the Visa approach for applying exemptions.

	of exemptions	
4.3.1	Merchant/Acquirer SCA/exemption process flows	<p>Figure 17 amended to:</p> <ol style="list-style-type: none"> <li>1) Remove anonymous transactions as merchants and Acquirers cannot recognize these</li> <li>2) Clarify OLO definition</li> <li>3) Include reference to secure corporate payments exemption</li> <li>4) Clarify that TRA exemption should be applied in preference to low value exemption</li> <li>5) Clarify that Visa does not support the recurring transactions exemption</li> <li>6) Clarify the way the trusted beneficiaries exemption is supported by VTL and update terminology</li> </ol>
4.3.2	Issuer Key decision points	<p>Figure 18 updated:</p> <ol style="list-style-type: none"> <li>1) To correct error in labelling</li> <li>2) Add scenario of unflagged transactions received direct to authorization</li> </ol> <p>Fig 19 updated:</p> <ol style="list-style-type: none"> <li>1) To clarify handling of unflagged transactions received straight to authorization</li> <li>2) To state that the recurring transactions exemption is not supported by Visa</li> <li>3) Reference the secure corporate payments exemption</li> <li>4) Clarify that the low value exemption should not be applied to zero value transactions</li> </ol>
4.4	Liability for fraud-related disputes	Addition of guidance that disputes liability under Visa Rules may differ from regulatory liabilities under PSD2.
4.4	Liability for fraud-related disputes	Clarification note added to Table 26 and information added on anonymous cards.
4.5.1	The low value exemption	Additional information added on requirements on Issuers regarding incrementing the velocity counters and applying SCA when required.

4.5.2.4	Qualification to apply the TRA exemption	Clarification added that only the PSP applying the exemption needs to have a fraud rate within the reference fraud rate.
4.5.3	Application of the trusted beneficiaries exemption	<p>Wording changed to clarify:</p> <ul style="list-style-type: none"> <li>• The regulatory conditions governing the application of the exemption</li> <li>• Qualification and technical dependencies for Visa Trusted Listing</li> <li>• Liabilities and disputes</li> <li>• Application by agents and marketplace platforms</li> <li>• Application of the exemption through the VTL program</li> </ul>
4.5.4	Secure Corporate Payment Processes and Protocols Exemption	Addition of new guidance on the interpretation and principles for the application of the secure corporate payment exemption.
4.6.1.2	Issuer selection and deployment of EMV 3DS challenge methods - The development of inclusive strategies	<ul style="list-style-type: none"> <li>• Addition of information on Visa proposed approach for authentication methods and factors following EBA opinion published 21<sup>st</sup> June 2019</li> <li>• Table 31 updated to reflect position on factors in EBA opinion published 21<sup>st</sup> June 2019</li> </ul>
4.6.1.3	Guidance to Issuers on populating the 3DS challenge Window	Addition of guidance on content to be included in the 3DS challenge window.
4.6.1.4	Out of band biometrics	Additional guidelines added on considerations for implementing OOB biometric authentication solutions.
4.6.2	Honoring step-up authentication requests	Additional information added on the requirement for Issuers to apply SCA when requested by merchants notably when establishing MIT agreements.
4.6.3	3RI authentication requests	Additional information added on 3RI authentication requests.
4.6.4.1	Issuer processing guidelines: BIN verification	Information added on use by Issuers of BIN verification to identify out of scope transactions and some transactions that qualify for an exemption.

4.6.4.2	Issuer processing guidelines: Zero value authorizations	Additional information provided on: <ul style="list-style-type: none"> <li>• merchants requesting SCA</li> <li>• not incrementing low value counters for zero value authorizations</li> <li>• setting up Stored Credentials</li> <li>• setting up MIT agreements</li> <li>• Table 29 reformatted, retitled and more information added</li> </ul>
4.6.4.3	Inclusion of CAVV and TAVV in MIT transactions	Additional information provided on resubmissions in mass transit use cases.
4.6.4.4	Reauthorizations	Section reworded to clarify why Reauthorizations can use exemptions and may include a CAVV.
4.6.4.5	Identification of transactions in accordance of the MIT framework	Clarification added on Issuer identification and MITs under the Visa MIT Framework.
4.6.4.9	Making allowances for legitimate data variations	Additional guidance to Issuers added to highlight that there will be legitimate variations in transaction data between authentication and authorization or between CITs establishing mandates and subsequent MITs.
4.6.5	Handling transactions from merchants who are not prepared for PSD2 or incorrectly submit transactions	Addition of guidance on handling incorrectly submitted transactions from merchants who are not fully prepared for PSD2.
4.7.2	STIP	Guidance updated to align with current STIP VBN.
4.8	Visa Direct and SCA under PSD2	New section added describing Visa Direct and providing guidance on when SCA is and is not required for Visa Direct transactions.
4.9	Visa Checkout and Visa Secure Remote Commerce	New section added providing information of Visa Checkout and migration to Visa Secure Remote Commerce.
4.10	Visa Secure Authentication Technology and non-Visa Transactions	New section added giving guidance on submission of non-Visa transactions via Visa authentication technology.
5.1	Inclusion of authentication-related data	New section added to capture common repeating patterns in the scenarios to clarify best practice with regards to the inclusion of

		authentication related data in authorizations and Reauthorizations. Other scenarios throughout section 5 have been modified to point to content in this section 5.1 where relevant. This change has been made for clarity only. The steps of existing scenarios throughout section 5 have not been changed unless otherwise indicated.
5.1.1	Cardholder-Initiated Transactions (CITs)	News section added summarizing use of indicators, CAVV and TAVV for PAN and token CITs.
5.1.2	Cardholder-Initiated Transactions (CITs)	New section added confirming that MITs are out of scope of SCA, that authentication data is not required, and that Issuers may not decline MITs with a response code 1A.
5.1.3	Reauthorization MIT	New section added covered use of authentication data, CAVV & TAVV in the context of Reauthorization MITs.
5.2	One-time purchase scenario	Information on use of authentication data clarified.
5.3.1	Delayed Shipment – expected delay	Scenario steps clarified (authentication of the customer, performing zero-value account verification and submitting delayed authorization).
5.3.2	Delayed Shipment – unexpected delay	Scenario steps clarified (authentication of the customer, submitting reversal and submitting delayed authorization).
5.4.1	Split Shipment – all fulfilled within 7 days	Scenario steps clarified (authentication of the customer, submitting authorization and clearing of funds for each shipment).
5.4.2	Split Shipment – partially fulfilled within 7 days (unexpected delay)	Scenario steps clarified (authentication of the customer, submitting authorization and clearing of funds for each shipment, submission of reversal, submission of delayed authorization and clearing of funds for delayed transactions).
5.4.3	Split Shipment – Multiple Authorizations	Scenario steps clarified (authentication of the customer, submitting authorization/performing zero value account verification,



		submission of delayed authorization and clearing of funds).
5.5	Open orders unknown amount	Scenario options clarified (authentication and authorization steps and use of authentication data).
5.5.3	Open orders unknown amount Option 3	Option 3 "Process using MIT Unscheduled Subscription type (UCOF)" changed to "Authenticate and use Incremental MIT to authorize amount above initial amount". Merchants cannot perform this type of transaction using a UCOF MIT but can perform an incremental MIT for an additional amount above the initially estimated transaction value.
5.6.2	Aggregated Payments Option 2: Authentication for fraud liability protection	Clarifications to made to step 3 (perform a zero-value account verification) and to step 4 (merchant response to an authorization decline received when the goods or services have already been provided) to correct inaccurate information provide in version 1.1 of this guide.  Change to the mechanism for merchant response to a decline when the goods or services have already been provided.
5.7.1	Real-time service via mobile app with payment after service /completion – Option 1: Direct to authorization flow	Scenario steps clarified (authorizing transaction, authentication of the customer if Issuer responds with response code 1A, submission of reversal and authorization for final amount).
5.7.2	Real-time service via mobile app with payment after service /completion – Option 2: Perform authentication every time	Scenario steps clarified (authentication of the customer, including communicating with the customer that they are being authenticated for the maximum amount; authorization/performing zero-value account verification; authorization of final amount using exemption or new authentication; submission of delayed authorization and clearing of funds).
5.7.3	Authenticate and use Incremental MITs to authorize amount above initial amount	A new option using incremental MITs has been added for the scenario where a real time service is delivered with payment due after service completion.
5.9	Resubmissions	Additional text added to clarify that this Resubmission MIT type only applies in a contactless transit environment and

		clarification of scenario in which resubmissions must not be used.
5.10	Accessing stored credentials using QR Codes	New use case added.
5.11	Establishing a new agreement for future MITs	Clarification on amount that the merchant must authenticate and authorize on setting up an MIT agreement and on disclosure of T&Cs.
5.11.1	Establishing a new agreement for future MITs - SCA is required by merchants to set up new agreement	Clarification of scenario steps (authentication of the customer, authorization of the transaction, authorization using the MIT Framework, clearing of funds).
5.11.4	Agreements established prior to PSD2 RTS for SCA coming into effect	Clarification on use of Acquirer assigned interim Transaction ID where the merchant does not have a prior Transaction ID available.
5.13	Executing payments based on established agreements	Clarification added that MITs are out of scope of SCA.
5.13.1	Installments and prepayments	Clarification of definition made, and scenario expanded to cover prepayments (e.g. where a down-payment is made for goods at time of purchase followed by the balance payment at a later date) as well as installments.
5.13.2	Subscriptions are fixed interval	Clarification provided on amount to authenticate and authorize when agreement is set up & scenario steps clarified, notably authorization using the MIT Framework.
5.13.3	Signing up for services charged at irregular intervals (usage based)	Scenario steps clarified, notably authorization using the MIT Framework.
5.13.4	Processing a purchase at the same time as establishing a new agreement	Scenario steps clarified, (Authentication of the customer, authorization process options, authorization using the MIT framework and clearing of funds).
5.14	Visa Direct payment	Section added to explain how to apply SCA to various scenarios using Visa Direct using OCTs and AFTs.
5.15	B2B payments	Section added to explaining practical steps for applying the secure corporate payments

		exemption and use of the Secure Corporate Payment Indicator for B2B payments.
5.16.2	Multiparty Commerce – marketplaces (single merchant)	Addition of note clarifying that an entity that brings customers and merchants together but does not handle payments on behalf of the merchant is not considered a Marketplace under Visa Rules but a referral service.
5.16.4	Referral Service	Clarifications made to the application of SCA for Referral Services.
5.18.1	Non-financial scenarios - Adding a card to a merchant account/customer profile	Clarifications made to scenario steps (disclosure of use of stored credential, obtaining cardholder consent, authenticating the customer if there is a risk of fraud and performing a zero-value account verification).
5.18.2	Non-financial scenarios - Adding a card to an account during a purchase	Clarifications made to scenario steps (disclosure of use of stored credential, obtaining cardholder consent, authenticating the customer, authorizing the transaction).
5.18.4	Non-financial scenarios – Card details updated by the Issuer	Definition of use case clarified to include an Issuer switching their card portfolio to Visa from another scheme.
5.18.5	Non-financial scenarios – Cardholder switching Issuers under the UK Account Switch Service	New section added to explain implications for SCA on the UK Account Switch Service.
5.18.7	Non-financial scenarios – Card details updated by the Customer	Text clarified to state that SCA is required when the customer changes details and there is a risk of fraud.
6.1	Issuer planning checklist	Activities re-ordered to place emphasis on support of latest technologies to optimize for PSD2 and requirements to adopt EMV 3DS2.2.1 and EMV 3DS 2.2.0 and RBA.
6.1	Issuer planning checklist	Addition of new activity on development of policies for dealing with transactions from merchants that are not fully prepared for PSD2.
6.1	Issuer planning checklist	Section amended to take account of roadmap for introducing SCA methods that use compliant factors, and requirements for

		implementation planning and reporting following the EBA opinions published 21 June 2019 and 16 October 2019.
6.2	Acquirer Planning Checklist	Section updated to reflect the requirement on Acquirers to migrate all their merchants to solutions that support PSD2 SCA as required by the EBA opinions published 21 June 2019 and 16 October 2019.
6.2	Acquirer Planning Checklist	Timescale for support of 3DS2.0 changed from September 2019 to “as early as possible”.
7	Bibliography	Updating of bibliography to add reference to newly published supporting guidance.
Glossary	Glossary	Addition of glossary of terms.
A.2 Appendix 2	Table 42 Visa Authentication messages, message values and how they are used	Table retitled to correct error.
Appendix 3 guide version 1.1)	Rules detail	Appendix removed.
A.3 Appendix 3	Considerations for Implementing OOB Biometrics on 3-D Secure 2.1 and 2.2	New Appendix added summarizing the support of OOB Biometrics for each version and summarizing the UX stages and considerations with sample screen shots.
A.7Appendix 7	EEA Countries in scope of PSD2 SCA	Guidance added on non-EEA territories where PSD2 may be applied under local law.



# 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) 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 compliance 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, remote and m-payments - within the European Economic Area (EEA<sup>1</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 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 SCA. The EBA has subsequently confirmed<sup>2</sup> that the requirements of PSD2 SCA apply as of 14 September 2019 and that the deadline by which the period of supervisory flexibility should end is 31 December 2020. The migration plans of PSPs, including the implementation and testing by merchants should also be completed by 31 December 2020.

The EBA has published a set of milestones and expected actions from National Competent Authorities (NCAs) towards issuing and acquiring PSPs. These include:

- Provision by PSPs of specific information and reporting on their authentication approaches and implementation progress
- NCAs taking stock of PSP readiness and progress
- Provision of information by PSPs to customers and merchants
- Completion of PSP implementation plans

Visa has collaborated with the industry to recommend a consistent transition period to be applied across all member states.

---

<sup>1</sup> For more information on the territories the requirement applies to please see Appendix 7

<sup>2</sup> Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions 16 October 2019

In the meantime, Visa has co-signed a European Payments Industry (EPIF) statement<sup>3</sup> advising all Issuers to continue authorizing transactions, in the same way they have previously done, after 14 September 2019. This is to avoid disruption to e-commerce and European payments and is in response to the EBA guidance.

Issuers will be expected to continue to use legacy solutions for authentication and fraud mitigation strategies.

Visa will be actively monitoring authorization responses to identify Issuers that are reporting an increased number of declines – working with them to find solutions that allow customers to make seamless payments. Visa will also use its overview of the payments ecosystem to inform local regulators around the impact of SCA on European payments.

Visa will continue to work with the whole industry on addressing the challenges of readiness and meeting the milestones in the SCA roadmap.

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.

**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.

The EBA Opinion published 21<sup>st</sup> Jun 2019<sup>4</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

<sup>3</sup>For details see: <https://paymentinstitutions.eu/pressroom/joint-industry-statement-on-sca-implementation/>

<sup>4</sup> Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2 21 June 2019

- An OTP cannot be used as a knowledge element but may be used as a possession element

SMS OTP used alongside card details is however an approach that has previously been widely implemented by Issuers as a practical and inclusive SCA approach.

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 authentication methods:

### 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 will use 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 Risk Based Authentication

Visa is exploring ways to enhance 3DS to incorporate behavioral biometrics into the data provided through 3DS. This will enable a compliant SCA solution using an OTP as evidence of possession and the behavioral biometric as evidence of inherence.

Biometric solutions will take time to develop, implement and deploy to cardholders. On this basis, Visa is working with regulatory authorities to request additional time for to allow a properly managed migration from SMS OTP in conjunction with 3DS and card data.

### 2.1.3 Other OTP Solutions

Other OTP solutions 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, or an inherence factor such as a biometric, can provide inclusivity solutions for customers unable to authenticate via a mobile phone.

## 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, 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 card payments, set out in Table 2.

**Table 2: Specific Fraud Thresholds for 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 €30 do not require SCA up to a maximum of 5 consecutive transactions or a cumulative limit of €100.

### 2.2.3 Trusted beneficiaries

Visa cardholders may add a merchant to a list of “trusted beneficiaries” held by their Issuer. Subsequent payments to such merchants do not require SCA.

### 2.2.4 Secure corporate payments

Payments made through dedicated corporate processes and protocols (e.g. lodge cards, central travel accounts and virtual cards) which are initiated by business entities, not available to consumers and which already offer high levels of protection from fraud may be exempted from SCA, subject to the view of the relevant competent authorities.

Lodge Cards, Central Travel Accounts and Virtual Cards that are not associated with an individual cardholder and are used within a secure dedicated corporate payment process are examples that may fall into this category.

### 2.2.5 Recurring Transactions

Please note Visa does not consider the recurring transactions exemption to be applicable to Visa card transactions. Visa’s view is card transactions that would otherwise be covered by the recurring transaction exemption are typically Merchant Initiated Transactions (MITs) and are therefore out of scope of SCA.

## 2.3 Out of scope transactions

The following transaction types are out of scope of SCA:

- **Merchant Initiated Transactions (MITs)** - A transaction, or series of transactions, of a fixed or variable amount and fixed or variable intervals 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. These transactions are out of scope. Where the initial mandate is set up through a remote electronic channel, SCA is required in most cases but is not necessary for subsequent payments initiated by the merchant. This applies to all payment instruments including cards and tokens.
- **Mail Order/Telephone Order (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>5</sup>. However, SCA should still be applied on a “best efforts” basis.
- **Anonymous transactions** - Transactions through anonymous payment instruments are not subject to the SCA mandate, for example anonymous prepaid cards.

## 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.

## 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 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.

---

<sup>5</sup> Refer to Appendix A.7 for a list of EEA countries

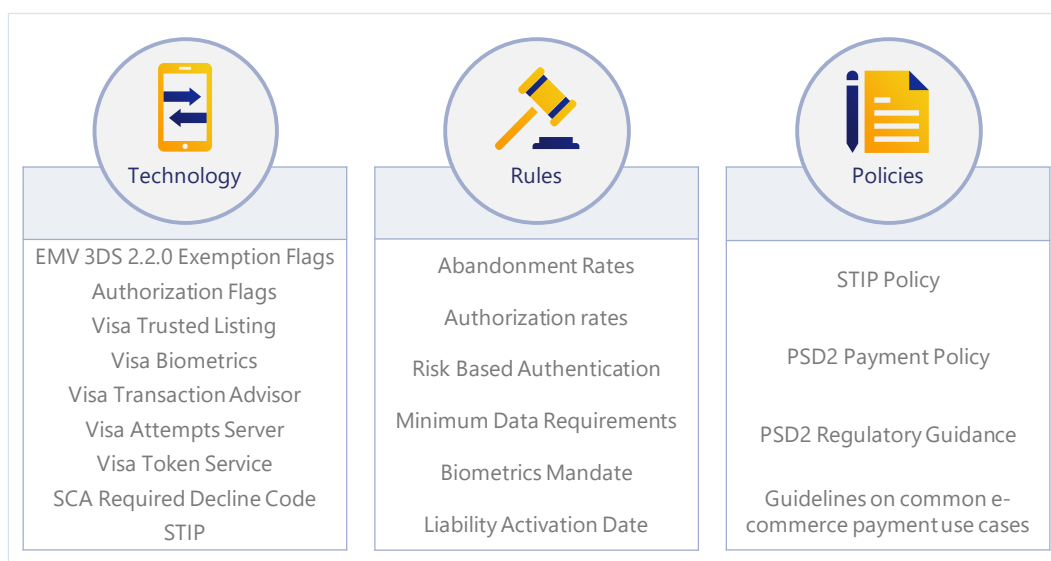
# 3. Visa's PSD2 solutions

## 3.1 Solution summary



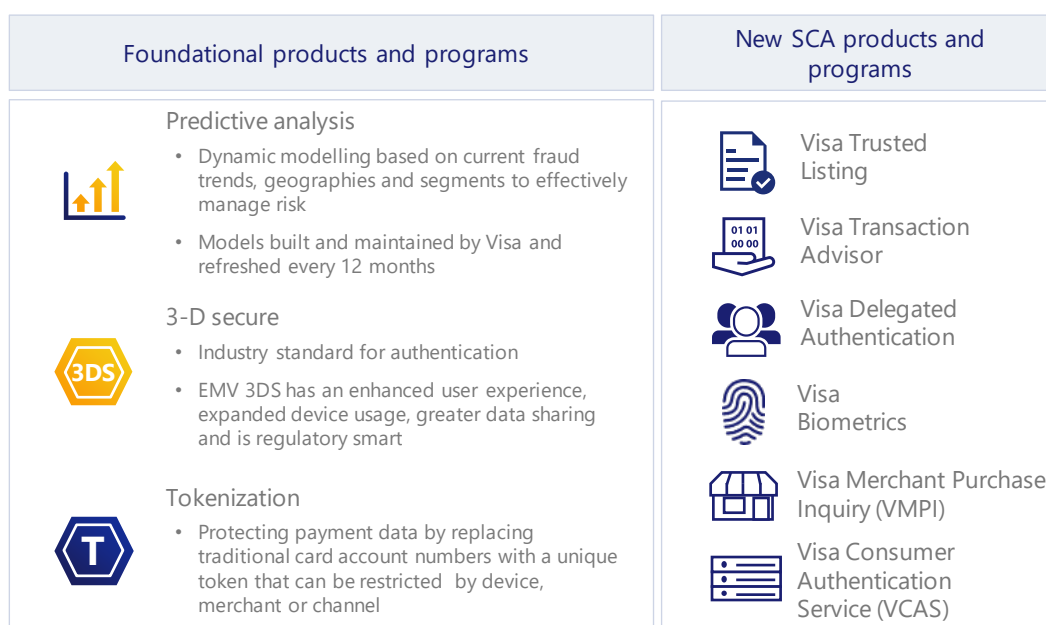
Visa is implementing a portfolio of solutions to help support the application of SCA and exemptions. These comprise a combination of technology solutions, enhanced rules and policies which are summarized in Figure 1 below.

**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 new products & programs**



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 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.

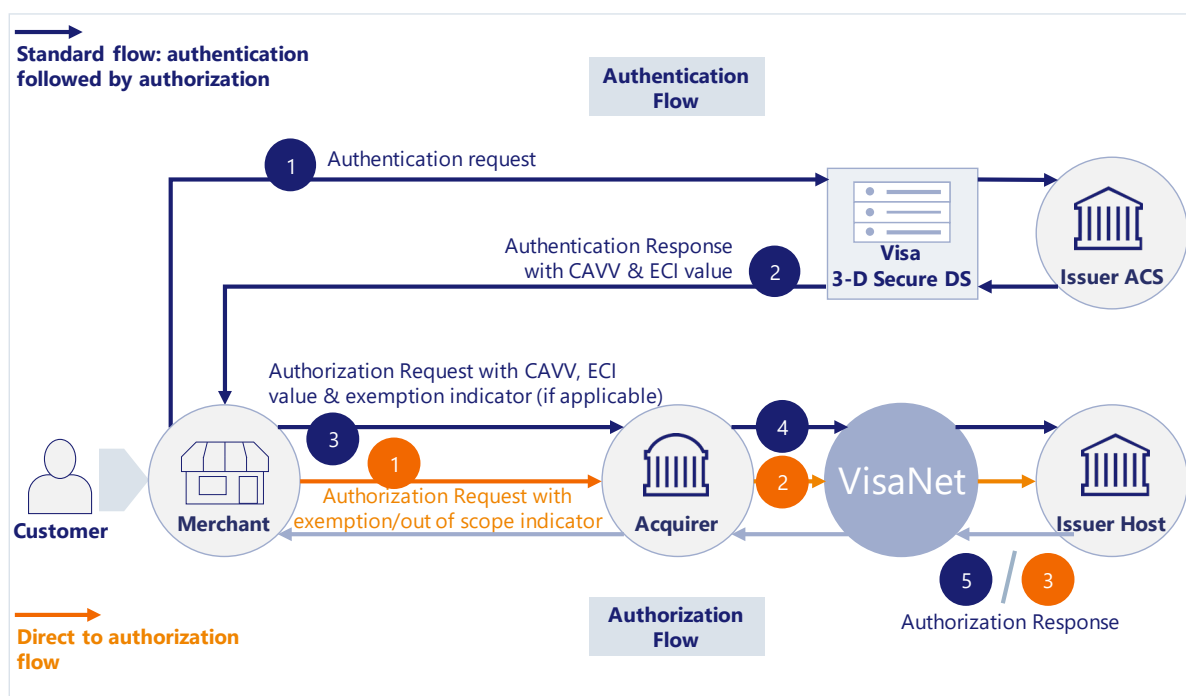
In a standard flow, merchants will submit a transaction for authentication, in some cases with an indicator requesting an exemption from SCA requirements. If the authentication is successful, the result will be returned along with a cryptogram (CAVV), and the merchant will submit the transaction to authorization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

Visa also supports the option for transactions to be submitted direct to authorization. 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

These basic flows are summarized in Fig 3 below:

**Fig 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



New indicators in the authorization request message will be used by Issuers to identify Acquirer exemptions. If a merchant would like to indicate that an Acquirer exemption is to be applied, an exemption flag 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

New indicators in the authorization request message can be used by merchants to indicate exemptions being applied for by Acquirers. 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 Cloud Token Framework under the Visa Delegated Authentication Program<sup>6</sup>) cryptograms are used to communicate the authentication status of the transaction. The messages work as summarized in Figures 4 & 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 Issuer 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>6</sup> For more information about the Cloud Token Framework see Section 3.4.1.2; about Visa Delegated Authentication Program see Section 3.8; and about authentication data if using 3-D Secure see Section 3.3.8

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

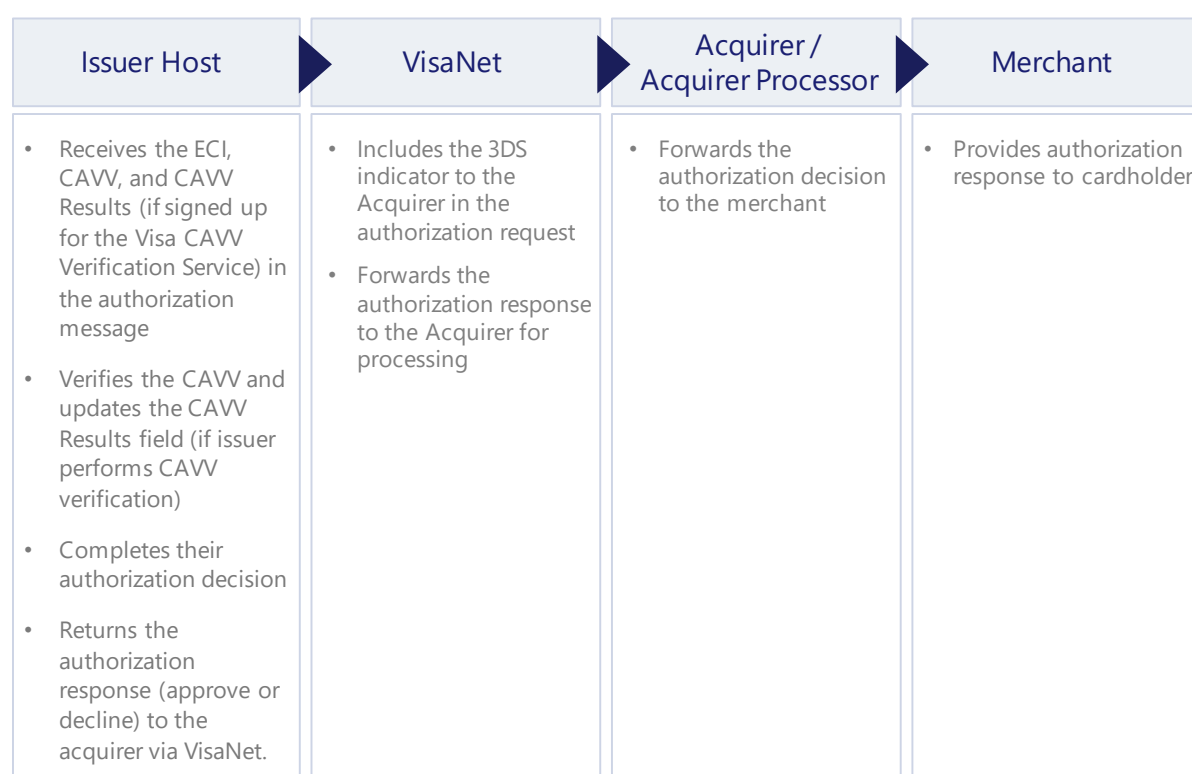


Table 3 summarizes the key relevant ECI values returned by 3DS. The format and role of the CAVV is summarized in more detail in Section 3.2.6.

**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**

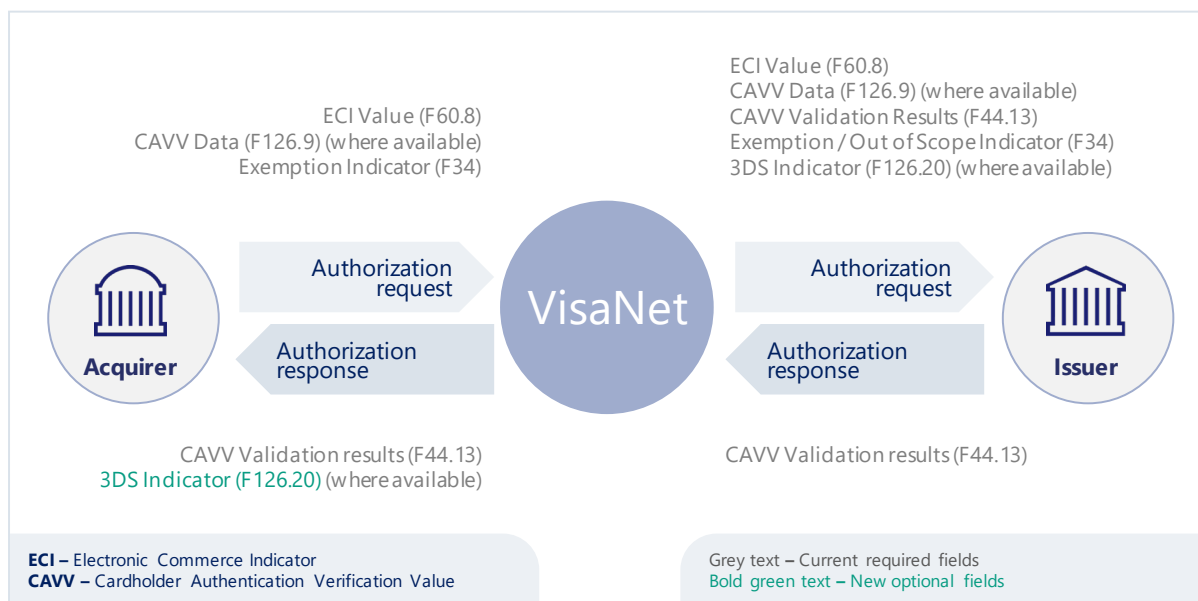
Field	Set by	Function	Field Value/Indicator
F19	Acquirer	Populated with the Acquiring Institution Country Code allowing the Issuer to determine whether the transaction is in or out of scope of SCA	Acquiring Institution Country Code
F25	Acquirer	Point-of-Service Condition Code – required for CAVV processing which in addition can be used to indicate MOTO transactions	Existing values as defined in the Visa technical specification <sup>7</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</p> <p>Allows Visa to indicate to Issuers that a transaction is an MIT out of scope of SCA</p>	<p>Effective 3 June 2019, the following tags are used to carry the SCA exemption indicators in the new Dataset ID 4A in existing TLV Field 34:</p> <ul style="list-style-type: none"> <li>• Tag 84 - Trusted Merchant Exemption Indicator</li> <li>• Tag 87 - Low Value Exemption Indicator</li> <li>• Tag 88 - Secure Corporate Payment (SCP) Indicator</li> <li>• Tag 89 - Transaction Risk Analysis (TRA) Exemption Indicator</li> <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>Effective 31 August 2019, the value of 1 in Tag 80, Dataset ID 02 in TLV Field 34 indicates a transaction is an MIT out of scope of SCA</p>
F39	Issuer	Response to F34 exemption request indicating additional customer authentication required	Response code 1A
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>7</sup>
F60.10	Acquirer	Indicates a transaction performed with an estimated amount	2 or 3
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>	Values 3900 to 3904

<sup>7</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
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	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 3.10.2.2 for more details
F126.13	Acquirer	Used to indicate (with F125) if the transaction is a Recurring, Installments/Prepayment or Unscheduled Credential on File out of scope MIT	Value R, I or C
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 Tables in Section 3.2.5
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**







Visa is implementing a new field, Field 34, to support PSD2 SCA requirements by indicating an Acquirer applied exemption. Additionally, a new response code 1A in Field 39 will be available to Issuers to indicate that the transaction cannot be approved until SCA is applied.

#### Requirement

Visa requires that Acquirers specify only one SCA exemption indicator per authorization request.

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, Visa requires that Acquirers 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.

Effective 3 June 2019 new tags listed in Table 4 above, are used to carry the SCA exemption indicators in the Field 34 Dataset ID 4A. These new 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.

Acquirers and Issuers in the Europe region can choose to support these changes from the January 2019 release. Effective with the October 2019 release, the changes will become mandatory for Acquirers and Issuers in the Europe region<sup>8</sup>. 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 by October 2019.

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

Table 5 provides a simple summary of the indicators for the key exemptions.

<sup>8</sup> Visa Mandate Article 9.1.3 See *Changes to Support New Tags and Mandate to Support Strong Customer Authentication Requirements Oct 19-533* for more details

**Table 5: Summary of Field 34 and EMV 3DS 2.2.0 indicators for exemptions**

Exemption	Acquirer or Issuer applied	EMV 3DS 2.2.0 Indicator Yes or No	ECI Value	Field 34 Yes or No	Visa or Acquirer Populated
Transaction Risk Analysis	Acquirer	Yes	7	Yes	Acquirer
	Issuer	No	5	No	N/A
Low Value	Acquirer	No	7	Yes	Acquirer
Secure Corporate Payment	Issuer	No	7	Yes	Acquirer
Trusted Beneficiaries	Issuer	Yes	7	Yes	N/A

### 3.2.3.1 Impact for Acquirers



Acquirers in the Europe region must be able to:

1. Support the new Field 34—Electronic Commerce Data, Dataset ID 4A—Supplemental Data in TLV format with new tags to indicate whether an e-commerce transaction is exempt from the PSD2/RTS SCA mandate
2. Receive the response code 1A (Additional customer authentication required) in existing Field 39

Response code 1A (SCA required) will be converted to 05 (Do not honor) in Field 39 if the Acquirer's parameter is not activated in VisaNet to receive the response code 1A.

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 new response code 1A 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 response code 1A when a transaction has been declined due to the absence of SCA
3. Not use response code 1A for a transaction that is out of scope of SCA

Issuers may respond with the new response code 1A 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 response code 1A for all transactions out of scope of SCA or not requiring SCA.

1. 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 but if SCA is not present in a transaction, the Issuer cannot decline on that basis
2. 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 response code 1A please see section 3.5.1. For information on identification of transactions that do not require SCA see sections 3.2.8 and 4.6.4.2.

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



Effective 31 August 2019, Visa has introduced a new indicator<sup>9</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.

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 3.10 for more details.

An Issuer activated to receive F34 will start to receive this value from 31 August 2019. If activated after that date, the value will automatically be received when present.

This enables Issuers to recognize a transaction as an MIT out of scope 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 3.10 for more details.

An Issuer must not use a response code of 1A 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.

---

<sup>9</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.

### 3.2.5 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 6 below.

**Table 6: The values for Field 126.20**

3DS Indicator Value	3DS Description
0	3DS 1.0.2 or prior all authentication methods
1	EMV 3DSChallenge flow using Static Passcode
2	EMV 3DSChallenge flow using OTP via SMS method
3	EMV 3DSChallenge flow using OTP via key fob or card reader method
4	EMV 3DSChallenge flow using OTP via App method
5	EMV 3DSChallenge flow using OTP via any other method
6	EMV 3DSChallenge flow using KBA method
7	EMV 3DSChallenge flow using OOB with Biometric method
8	EMV 3DSChallenge flow using OOB with App login method
9	EMV 3DSChallenge flow using OOB with any other method
A	EMV 3DSChallenge flow using any other authentication method
B	3DS unrecognized authentication method
D	EMV 3DSFrictionless flow, RBA Review
E	EMV 3DSAttempts Server responding
F	EMV 3DSFrictionless flow, RBA

### 3.2.6 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.

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

Visa will be enhancing the CAVV in the near future to support new 3DS use cases, multiple authentication methods, a merchant identifier, etc.

#### 3.2.6.1 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.

### 3.2.6.2 CAVV / TAVV Data in Field 126.9

Field 126.9 allows Acquirers to:

- 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.

### 3.2.6.3 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*.

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

### 3.2.7 Non-authenticated secure transaction with 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.

### 3.2.8 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>10</sup>
- Anonymous transactions

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

---

<sup>10</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	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: <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)	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 flag (value 1) in Tag 80, dataset 2 of Field 34 <sup>11</sup>
One-Leg-Out (OLO)	In the Visa processing system, these transactions are recognized by: <ul style="list-style-type: none"> <li>• An Issuer BIN outside of the EEA, or</li> <li>• An Acquirer location outside of the EEA (Field 19 – Acquiring Institution Country Code)</li> </ul> <p>Note that in these cases, SCA should still be applied on a ‘best effort’ basis so SCA may be present.</p>
Anonymous	Transactions performed with anonymous cards are out of scope of SCA; however, they cannot be recognized as such by merchants. In this case, the following approaches are possible: <ul style="list-style-type: none"> <li>• If the Merchant proceeds via authentication route, either requesting an applicable exemption or simple authentication and the card is not enrolled in 3DS, the response will be an ECI 7 and “Not Authenticated/Account Not Verified” message. <ul style="list-style-type: none"> <li>• From Sept. 2019 a transaction status response code will be sent with a code 87 “Transaction is excluded from Attempts Processing e.g. non-reloadable, TRA, etc.”</li> </ul> </li> <li>• If merchant proceeds direct to authorization, then Issuers are being asked to recognize BINs of out of scope cards and, therefore, should not request SCA.</li> </ul>

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

<sup>11</sup> See Section 3.10 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 3.10.



**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 Response Code 1A (SCA required) 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 Sections 4.8 and 5.15. 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 4.6.4.2 to recognize scenarios where they should/should not request SCA when the transaction is of zero value.</p>

### 3.2.8.1 Acquirer impact

1. 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 and for non-ecommerce PAN key entered transactions, this means that without any MOTO or MIT indicators(s) these transactions may not be recognized by Issuers as MOTO or MIT out of scope transactions.
2. Transactions that are acquired in the EEA, even if the merchant is outside the EEA are considered in scope, and in this case, merchants should work with their Acquirer to ensure that SCA can be applied.
3. Acquirers are reminded to ensure that F19 is populated with the correct Acquiring Institution Country Code. 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.

### 3.2.8.2 Issuer Impacts

Issuers in the Europe region must:

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

- 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>12</sup>
2. Not use a response code 1A (SCA required), or equivalent, for authorization requests for transactions deemed out of scope from a regulatory perspective, specifically when a merchant is not able to obtain SCA for legitimate MITs, MOTO, or transactions performed with anonymous cards.<sup>13</sup>
  3. Identify transactions acquired outside the EEA through the Acquiring Institution Country Code in F19 of the authorization request, not by the merchant country code.

### 3.3 3-D Secure



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

3-D Secure provides a strong customer authentication solution that enables Issuers, Acquirers and merchants to provide 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.

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 will adopt 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>.

<sup>12</sup> For more information on the reception and use of the original Transaction ID please refer to Section 3.10.2.2.

<sup>13</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*

### 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

### 3.3.2 EMV 3DS implementation requirements & timescales



#### 3.3.2.1 The requirement to adopt EMV 3DS 2.2.0

EMV 3DS 2.2.0 provides key 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 2.2.0 across the ecosystem is an important step in achieving SCA regulatory compliance. Visa recognizes that all parties are moving at pace to implement the new 3DS versions. To help further those efforts, Visa is implementing a technology roadmap to help ensure smooth industry-wide deployment of EMV 3DS.

#### Best Practice

Merchants and Issuers are strongly advised to adopt EMV 3DS 2.2.0 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 2.2.0.

#### 3.3.2.2 EMV 3DS activation date

The European Banking Authority (EBA) has accepted that local regulators may decide to work with PSPs and other stakeholders and provide a transition period that allows more time for all parties to be ready. Visa has collaborated with the industry to recommend an 18-month transition period across all member states, which would provide sufficient time for all parties to make the necessary technical changes. Due to this, Visa is moving Europe's EMV 3DS activation date back to 14 March 2020<sup>14</sup>.

<sup>14</sup> Visa had previously set an activation date of 12 April 2019 however this has been moved back in recognition of the need for further time for ecosystem to prepare for adoption of EMV 3DS and the delay in enforcement.

### 3.3.2.3 Issuer implementation dates

Visa has introduced changes to 3-D Secure rules to support SCA compliance<sup>15</sup>

#### Requirement

Visa expects Issuers in Europe to deploy EMV 3DS 2.1.0 by **14 March 2020** and to deploy EMV 3DS 2.2.0 by **14 September 2020**.

### 3.3.2.4 EMV 3DS Merchant Liability Protection

Effective immediately, until 14 March 2020, merchants will receive fraud liability protection on fully authenticated EMV 3DS transactions. Merchants will not be able to send EMV 3DS requests to European Issuers that do not support EMV 3DS. These merchants should send 3DS 1.0 requests or process as ECI 07 non-authenticated transactions.

#### Key Point

Effective immediately through 13 March 2020, merchants will not be able to send EMV 3DS requests to European issuers that do not support EMV 3DS.

Effective 14 March 2020, merchants will receive fraud liability protection on both EMV 3DS authenticated transactions and on EMV 3DS attempted authentication transactions, when European Issuers are not live on EMV 3DS. At this point, all European Issuers are expected to be able to respond with an EMV 3DS authentication response.

**Table 9 Liability protection for EMV 3DS Transactions**

	Through 13 March 2020	Effective 14 March 2020
Fully Authenticated	Issuer liable	Issuer liable
Attempted Authentication	Not available, merchant liable	Issuer liable <sup>16</sup>

For more information on how merchants can identify the version of 3DS supported by an Issuer and liability protection refer to Section 3.3.14.

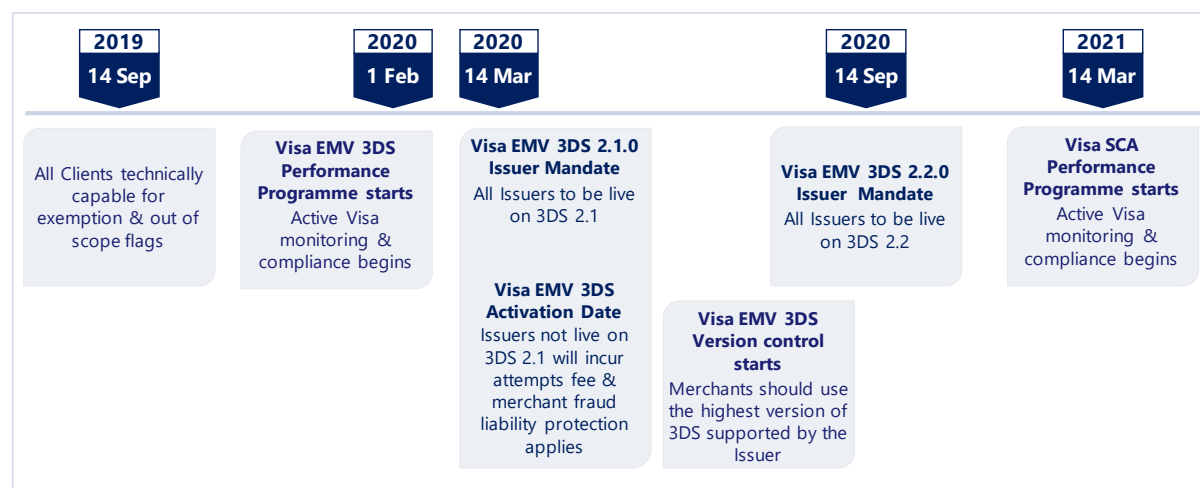
<sup>15</sup> See *Visa Business News: Important Changes to 3-D Secure Rules to Support Strong Customer Authentication Compliance*, 5 September 2019

<sup>16</sup> Authentication is routed to the Visa EMV 3DS Attempts server.

### 3.3.3 Visa roadmap for EMV 3DS implementation

Visa is implementing 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 10 provides a comparison of the main features of 3DS 1.0, EMV 3DS 2.1.0 and EMV 3DS 2.2.0.

**Table 10: 3DS version notable feature comparison**

Notable Features	3DS 1.0	3DS 2.1.0	3DS 2.2.0
SCA Compliant (2FA – static data, OTP)	Y	Y	Y
Dynamic linking - CAVV generated links authentication to the payment	Y <sup>17</sup>	Y	Y
Basic Issuer TRA (provided by the Issuer ACS)	Y	Y	Y
Mobile banking app integration	N	Basic	Y
Biometric authentication	N	Basic	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>18</sup>	Y
• Decoupled authentication	N	N	Y
Acquirer Exemption indicators			
• TRA performed prior to authentication	N	N	Y
• Trusted beneficiaries (whitelisting)	N	N	Y
Enhanced TRA plus data (100+ data elements)	N	Y	Y
Additional device compatibility e.g. gaming consoles	N	N	Y

Table 11 below shows the key features that are supported by different combinations of 3DS version support by Issuers and merchants and Tables 12 and 13 explain some of the key features of EMV 3DS 2.1.0 and EMV 3DS 2.2.0 in more detail.

<sup>17</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>18</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.

**Table 11 3DS Issuer and merchant version compatibility chart**

	Version	Issuer		
		3DS 1.0	EMV 3DS 2.1.0	EMV 3DS 2.2.0
Merchant	3DS 1.0	Merchant sends 3DS 1.0: <ul style="list-style-type: none"> <li>Basic SCA – no Acquirer requested exemptions</li> <li>Limited devices supported</li> </ul>	Merchant sends 3DS 1.0: <ul style="list-style-type: none"> <li>Basic SCA – no Acquirer requested exemptions</li> <li>Limited devices supported</li> </ul>	Merchant sends 3DS 1.0: <ul style="list-style-type: none"> <li>Basic SCA – no Acquirer requested exemptions</li> <li>Limited devices supported</li> </ul>
	EMV 3DS 2.1.0	Merchant downgrades to 1.0: <sup>19</sup> <ul style="list-style-type: none"> <li>Basic SCA – no Acquirer requested exemptions</li> <li>Limited devices supported</li> </ul>	Merchant sends 3DS 2.1.0: <ul style="list-style-type: none"> <li>Basic SCA – no Acquirer requested exemptions</li> <li>Supports all devices</li> <li>Poor out of band experience</li> </ul>	Merchant sends 3DS 2.1.0: <ul style="list-style-type: none"> <li>Basic SCA – no Acquirer requested exemptions</li> <li>Supports all devices</li> <li>Poor out of band experience</li> </ul>
	EMV 3DS 2.2.0	Merchant downgrades to 1.0: <sup>19</sup> <ul style="list-style-type: none"> <li>Basic SCA – no Acquirer requested exemptions</li> <li>Limited devices supported</li> </ul>	Merchant downgrades to 2.1.0: <ul style="list-style-type: none"> <li>Basic SCA – no Acquirer requested exemptions</li> <li>Supports all devices</li> <li>Poor out of band experience</li> </ul>	Merchant sends 3DS 2.2.0: <ul style="list-style-type: none"> <li>Supports all Issuer &amp; Acquirer exemptions</li> <li>Supports all devices</li> <li>Best out of band experience</li> <li>3RI for Payments</li> </ul>

Legacy
  Interim
  Optimum

**Table 12: Key enhancements on the 3DS v2.1.0 specification release**

EMV 3DS Specifications Version 2.1.0 – Released: October 2017   Live From: Q4 2018	
Notable Features	Feature description
3DS Requestor Initiated (3RI) Messages	A channel that allows the merchant to initiate the authentication request without the cardholder being in-session
Support of App based purchases	Supports app-based purchases on mobile and other consumer devices
Checkout Integration	Enables merchants to integrate authentication into their checkout process for both app and browser-based implementations
Enriched data	Provides enriched data to support frictionless transactions
Challenge method support	Supports multiple options for step-up authentication
ID&V	Enables merchant-initiated account verification

<sup>19</sup> In the case that the merchant is unable to submit a 3DS 1.0 authentication request, or that the 3DS 1.0 authentication experience offered by the Issuer is likely to result in transaction abandonment, the merchant may fall back to non-secure e-commerce ECI 07 (provided this is permitted by regulation).

**Table 13: Key enhancements in the EMV 3DS v2.2.0 specification release**

EMV 3DS Specifications Version 2.2.0: Released December 2018, Live from Q4 2019	
Notable Features	Feature description
SCA/TRA Indicators	Indicate that Strong Consumer Authentication (SCA) or Transactional Risk Analysis (TRA) has already been performed prior to the authentication message being sent
FIDO <sup>20</sup> , Token, and Secure Remote Commerce (SRC) Data	Additional information as to how the cardholder logged in to their 3DS Requestor Account Specification has been updated to carry additional FIDO, token and SRC data from the merchant to the Issuer
Trusted beneficiaries exemption support	Support for enrollment at checkout and subsequent frictionless transactions
3DS Requestor Initiated (3RI) payments	This channel only supported non-payment transactions within v2.1.0 for account verification purposes only This channel has been expanded to payments in 2.2.0
Decoupled Authentication	A new authentication method which allows cardholder authentication to occur if the cardholder is off-line This authentication method can also be used if the cardholder is on-line via our Browser and App channels
Support of MOTO	3DS can be applied to MOTO transactions by utilizing 3RI and Decoupled Authentication
Improvements to the EMV 3DS Caching process (PReq/Pres cycles)	The PReq/Pres messages are utilized by the 3DS Server to cache information about the Protocol Version Numbers(s) supported by available ACSs, the DS, and also any URL to be used for the 3DS Method call

EMV 3DS 2.2.0 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 Appendix A.2 Table 51

<sup>20</sup> The FIDO Alliance is an open industry association focussed on developing strong authentication standards. For more information see <https://fidoalliance.org/>



### 3.3.4.1 3DS Requestor Initiated (3RI) payments

3DS Requestor Initiated (3RI) is a 3-D Secure transaction initiated by the 3DS Requestor for the purposes of confirming that an account is still valid or for Cardholder authentication. 3RI transactions enable merchants to obtain authentication data (CAVV, ECI) in the absence of the cardholder for transactions that have been previously authenticated. For Issuers, a 3RI transaction's prior transaction data improves risk management and provides secondary evaluation of a previously authenticated transaction. This feature allows merchants who have performed authentication for a transaction to maintain their fraud liability protection under legitimate circumstances, such as delayed or split shipments.

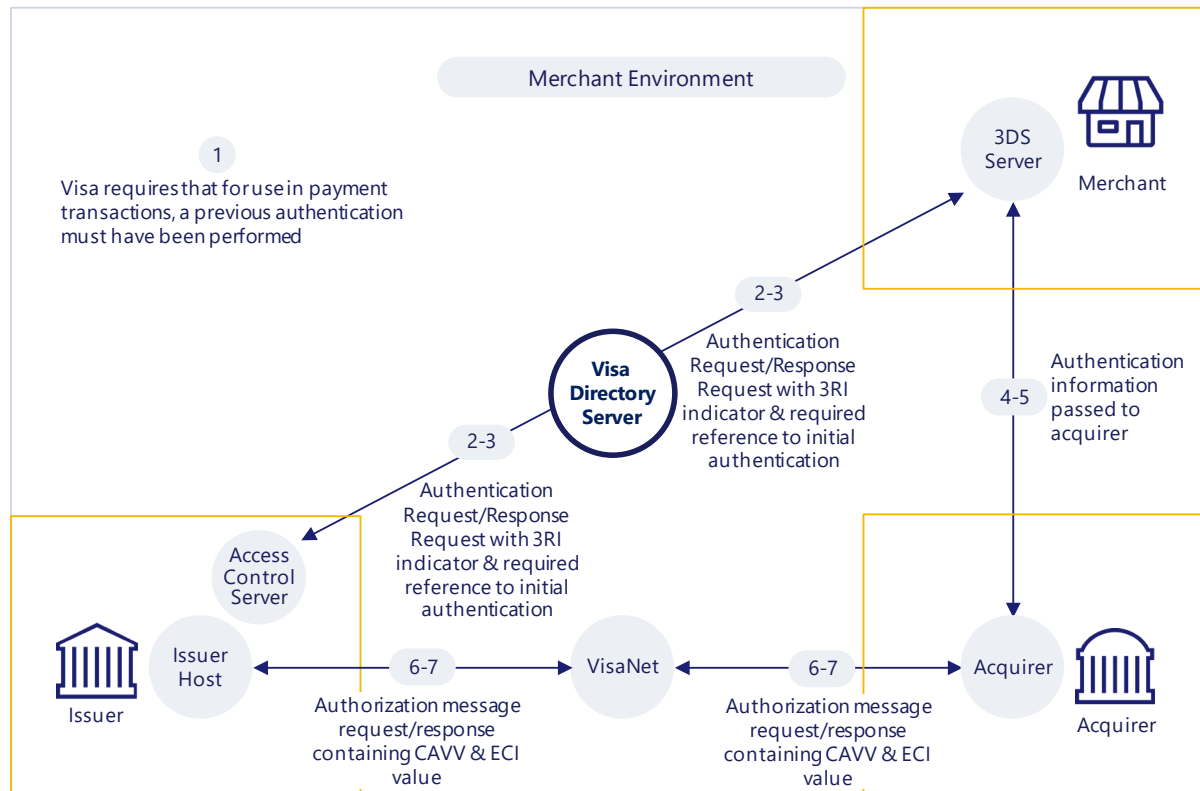
The feature can be used to enable merchants to effectively manage some complex payment use cases by for example:

- Allowing an authorized entity in a Multi-Party Commerce scenario to request a CAVV on behalf of a merchant
- Allowing a merchant to obtain a new CAVV in the case of a split or delayed shipment when one or more items are not ready for shipment until a much later date
- Requesting a new CAVV to maintain liability protection when authorization is sought more than 90 days after a transaction has been authenticated

Examples of where this may be used for specific transaction types are included in section 5.

Figure 8 below shows the standard 3RI flow.

**Figure 8: 3RI Flow**



Merchants and 3DS Server vendors should note the for 3RI transactions the 3DS Server should provide the following information:

- 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).

For more information on the application of 3RI please refer to sections 4.2.4 (Table 27 principle 3), 4.6.3 and 4.6.4.4.

### 3.3.5 EMV 3DS terminology



EMV 3DS differs in a number of ways from 3DS 1.0 and the terminology used has changed to reflect this.

**Table 14: Comparison of commonly used terms**

3DS 1.0 Term	EMV 3DS Term
Merchant	3DS Requestor (a merchant is an example)
Merchant Plug-in (MPI)	3DS Server
n/a	3DS Requestor Environment
Merchant Integrator	3DS Integrator
n/a	3DS Requestor App

### 3.3.6 EMV 3DS domains and components



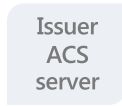


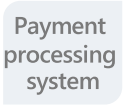

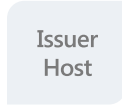


Visa's 3-D Secure 2.0 Program defines three distinct domains that interact to support authentication and authorization:

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

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

**Figure 9: Domains and components**

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

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 15: The role of the main components**

Component	Description
3DS Server	<p>The 3DS Server provides the functional interface between the 3DS Requestor Environment flows and the DS. The 3DS Server is responsible for:</p> <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 SDK	<p>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</p>
Directory Server (DS)	<p>The DS performs a number of functions that include:</p> <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>

Component	Description
Issuer Access Control Server (ACS)	<p>The ACS contains the authentication rules and is controlled by the Issuer. ACS functions include:</p> <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

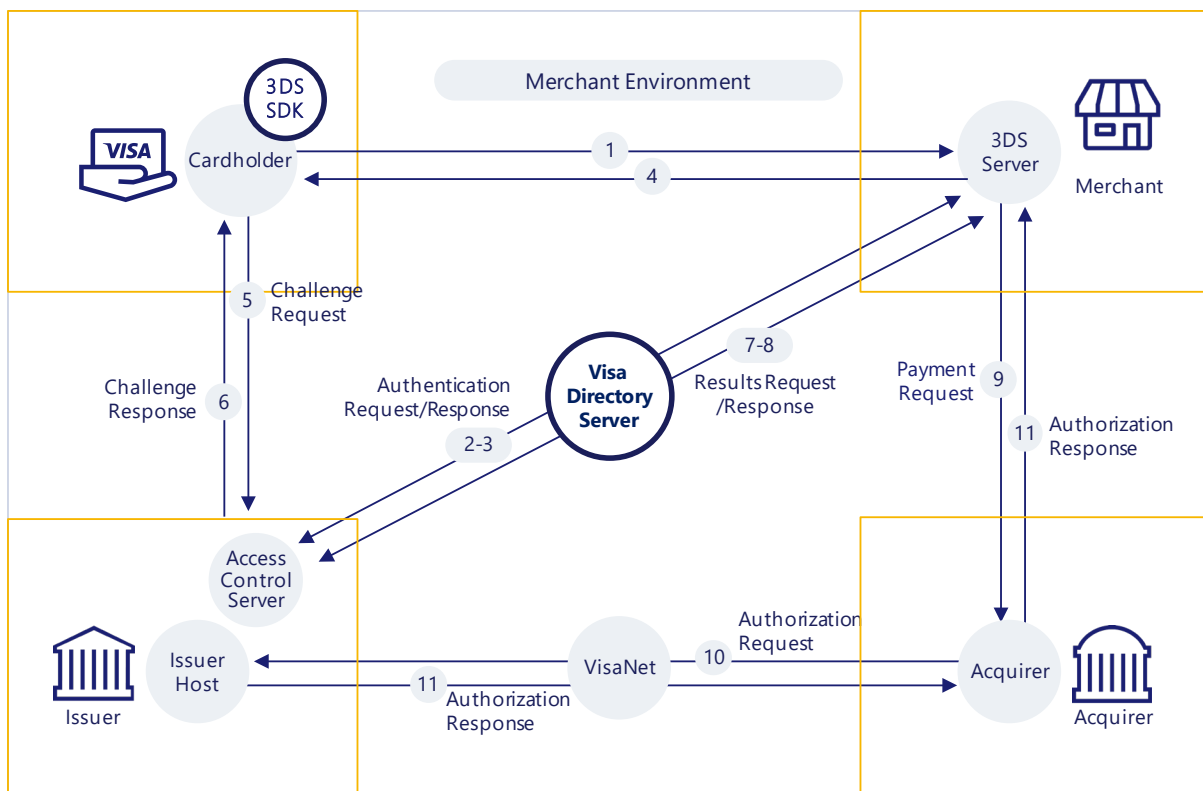
### 3.3.7 The EMV 3DS messages and process flow



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 an 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 flags 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 an 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 16 provides full details:

**Table 16: 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*.



#### 3.3.9.1 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 flag (3DS specification version 2.2.0 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 an 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. The data elements are listed in Appendix A.1. They 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, applying behavioral biometrics and/or undertaking RBA alongside the application of two independent SCA factors further strengthens the effectiveness of authentication. This is what Visa refers to as a “layered approach”.



The Data Element Types supported with EMV 3DS include:

**Table 17: 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>

### Requirement

Merchants are required to submit the required data elements listed in Appendix A.1 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 is introducing a rule to ensure that minimum data provision standards are applied. A complete list of data elements is at Appendix A.1.



### 3.3.11 Token transactions and 3DS



3DS authentication is supported for token-based, card on file, e-commerce, and application-based e-commerce transactions. 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 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

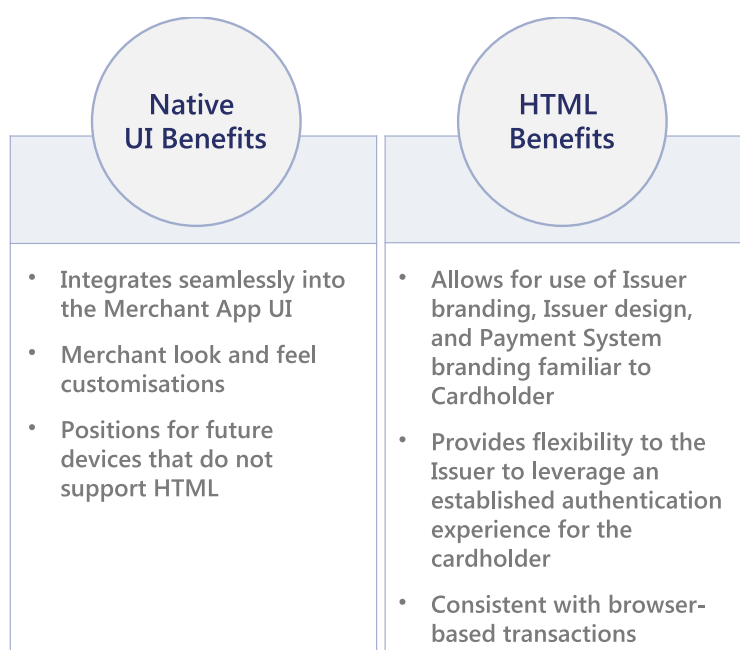


EMV 3DS provides significantly enhanced user experiences through:

- 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. Visa will provide best practice guidelines on the content of challenge messages. For more information please refer to Section 4.6.1 and to the 3DS UX Guidelines available on the Visa Developer Center.

### 3.3.13 EMV 3DS on different platforms



EMV 3DS has initially been specified to support desktop browser and mobile (HTML and native app) platforms. Future versions of the specification will extend support to other platforms including games consoles, allowing seamless support of in-game purchases.

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

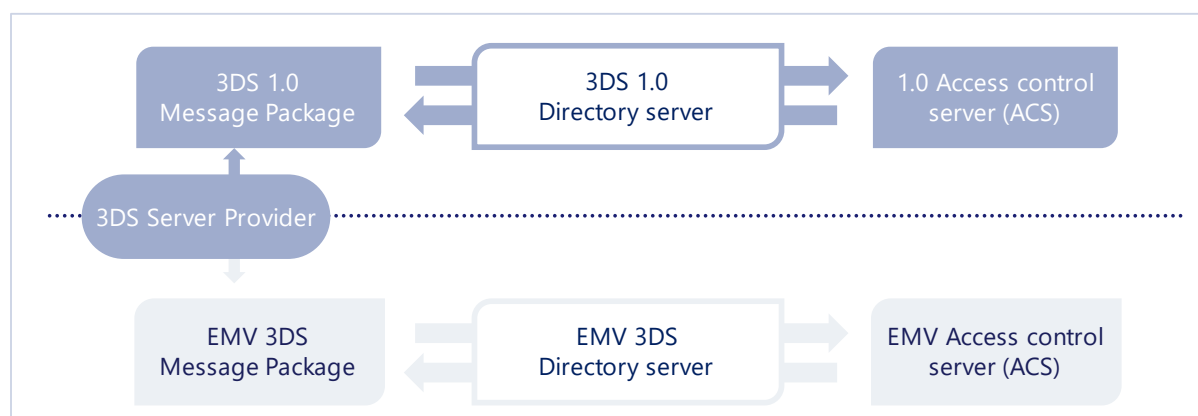


EMV 3DS and 3DS 1.0 are two separate, distinct protocols, supported by two separate Directory Servers that will co-exist independently in parallel for a transition period. Both protocols will continue to be supported until EMV 3DS reaches maturity in the market. Visa expects to announce a sunset date 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 receives a daily update from the Visa Directory Server stating the 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.

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



As stated in section 3.3.2.2, the Visa European activation date for EMV 3DS has been moved to 14 March 2020. From this date, merchants receive fraud liability protection for both successful and attempted 3DS transactions with both 3DS 1.0 and EMV 3DS.

It should be noted that after the activation date, a merchant that has upgraded to EMV 3DS will retain liability protection for an EMV 3DS authenticated transaction under the Visa Rules even if the Issuer does not support EMV 3DS.

In this case, if an Issuer's ACS is unable to respond to an EMV 3DS Authentication Request message, the Visa Attempts Server will respond. It provides a cryptogram to enable the merchant to prove they attempted authentication.

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

The potential combinations of responses and liabilities are summarized in Table 18 below.

**Table 18: 3DS transaction liability status after 14 March 2020**

Merchant 3DS Version	Issuer 3DS version	Issuer availability or Visa 3DS Attempts Stand In processing	Fraud liability under Visa Rules
3DS 1.0	3DS not supported	Visa Attempts Server	Issuer (ECI 06)
3DS 1.0	3DS 1.0	Issuer available	Issuer (ECI 05)
3DS 1.0	3DS 1.0	Issuer unavailable – Visa Attempts Server	Issuer (ECI 06)
EMV 3DS	EMV 3DS not supported (Issuer not supporting 3DS at all or supporting 3DS 1.0 only)	Visa Attempts Server	Issuer (ECI 06)
EMV 3DS	EMV 3DS	Issuer available	Issuer (ECI 05)
EMV 3DS	EMV 3DS	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.

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



Visa is implementing several solutions to help support the application of SCA and exemptions using the Visa Token Service (VTS). These solutions provide a complementary approach to the 3DS based solutions for clients wishing to build upon their tokenization strategies and platforms. This section briefly describes each of these solutions.

### 3.4.1 The Visa Token Service and the Cloud Token Framework

#### 3.4.1.1 The Visa Token Service (VTS)

VTS 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 token allows payments to be processed without exposing actual account details. VTS provides a complete integrated set of tokenization tools for merchants, Issuers, Acquirers and processors.

The VTS has been extended to address the requirements of PSD2 though:

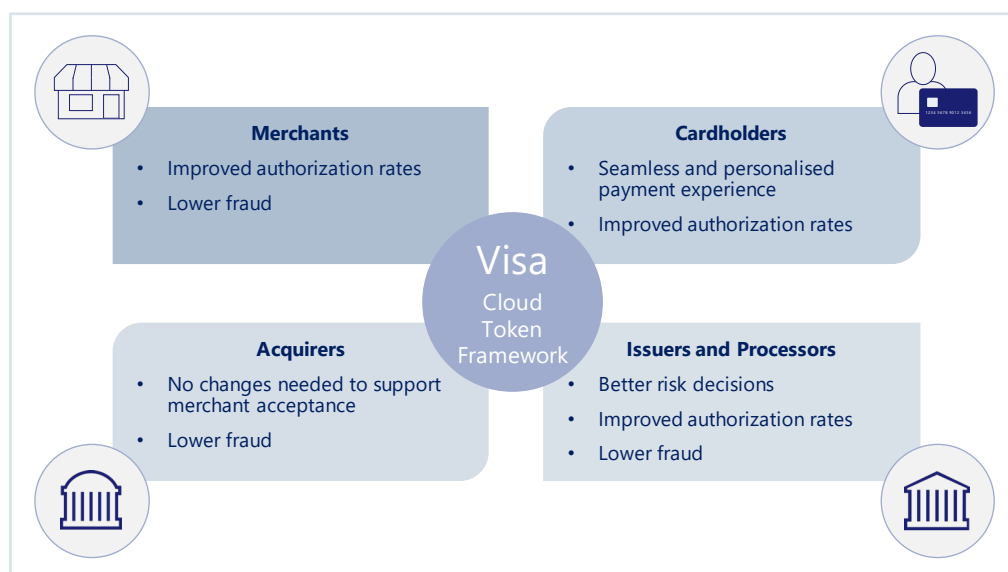
- Facilitating the application of SCA between customers and qualifying delegates participating in the Visa Delegated Authentication Program (see Section 3.8 below)
- Supporting dynamic linking through the token cryptogram
- Supporting the Visa Trusted Listing Program (see Section 3.6 below)

#### 3.4.1.2 The Visa Cloud Token Framework

The Cloud Token Framework is an enhancement to VTS 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.

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

**Figure 13: Cloud Token Framework Benefits**



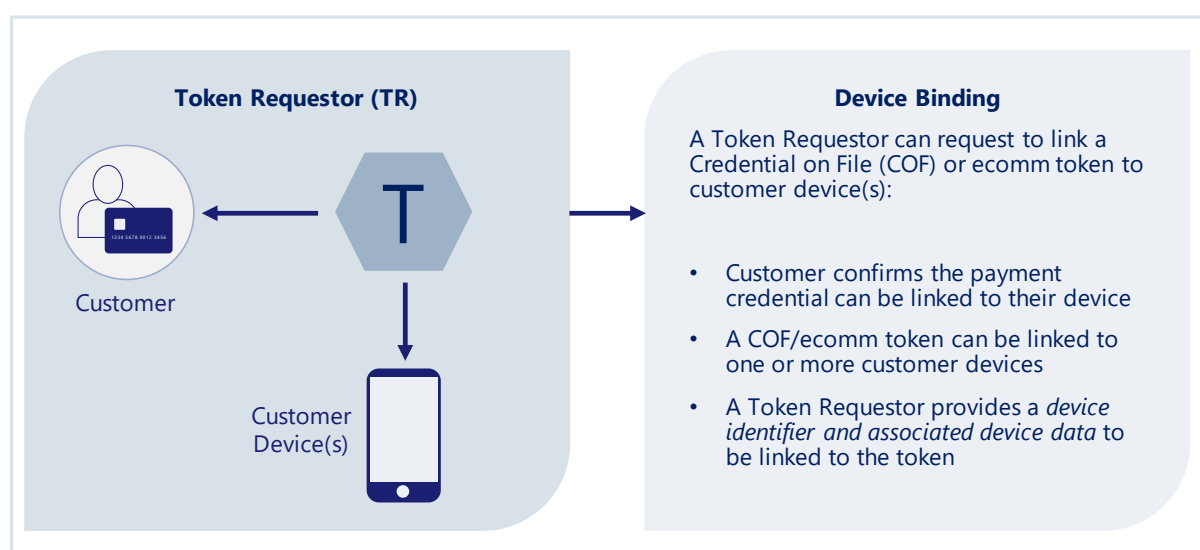
### 3.4.1.3 Features of the Cloud Token Framework

The Cloud Token Framework provides features to Issuers and Token Requestors (entities that request payment tokens for end-users, for example digital wallet providers, payment enablers or merchants) including:

#### 3.4.1.3.1 Device Binding

Device Binding links a token to a specific Token Requestor's device id and enables the linked device to subsequently satisfy the possession factor for SCA where the Token Requestor can reliably and unambiguously identify the device.

**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 two-factor authentication in order to verify the customer before the binding of the device to the token is finalized.

#### 3.4.1.3.2 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 use two independent factors.

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

Delegated authentication may be facilitated through account binding. This is the process of verifying that the merchant or wallet customer is also the Issuer's cardholder by performing Issuer authentication when binding is established. Account binding links a token to the Token

Requestor's customer and enables a customer's authentication into their merchant or wallet account to be used in the performance of SCA under the Delegated Authentication Program.

In order to support delegated authentication using tokens, VTS is also being enhanced to provide the following:

- A token-based cryptogram (TAVV) that will support dynamic linking between the merchant (payee) and the transaction amount using a verifiable authentication code
- The provision of indicators to the Issuer regarding which two authentication factors were performed by the delegate, plus the authentication amount (in addition to the authorization amount) and an identifier of the authentication payee to enable the Issuer to perform their own optional check on the dynamic elements of the transaction

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*.

### 3.5 Visa Rules & policies for PSD2 & 3DS



#### 3.5.1 Visa Rules relevant to PSD2 and 3DS

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
- Transactions that are out of scope of the SCA regulation or otherwise do not require an Issuer to apply SCA not being recognized
- SCA being requested when a customer is unable to authenticate a transaction
- 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, 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 summarized in Table 19.

**Table 19: Relevant rules summary** (\*subject to change)

**Important Note:** The Summary Description shown in Table 19 below is a brief summary of the main subject of relevant rules provided for information only. It is not, and should not be interpreted, as the text of the rule and in most cases does not provide a full description of the rule or conditions attached the rule. Readers must refer to the Visa document *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements* for the actual text of the rule because that document and the Visa Core Rules take precedence over this table in the case of conflict.

Rule	Number ID#	Summary Description
Application of SCA	0030622	In the Europe Region: A Member must ensure that Electronic Commerce Transactions initiated on Cards issued in the European Economic Area (EEA) and United Kingdom (UK) and acquired in the EEA and UK are subject to strong customer authentication in line with PSD2.
Issuer support of EMV 3DS 2.1.0 and EMV 3DS 2.2.0	N/A	Visa expects Issuers in Europe to deploy EMV 3DS 2.1.0 by 14 March 2020 and to deploy EMV 3DS 2.2.0 by 14 September 2020.
Use of SCA decline codes – exemptions & out of scope transactions	0029326	Visa Issuers must not systematically challenge transactions sent to authorization with an exemption flag or with a data element indicating that a transaction is out of scope.
Establishing Merchant Initiated Transactions	N/A	A merchant must request a SCA challenge when setting up an MIT series – subject to specific exceptions.
Honoring step up requests	N/A	Where a merchant requests an SCA challenge, an Issuer must respond to that request and ensure that the challenge is performed.
Use of Response Code 1A	N/A	An Issuer must only use a response code 1A (SCA required) where no other decline code is applicable, and only when SCA is required. If an Acquirer / merchant receives a response code 1A code in the authorization request, the merchant must ask the Issuer for a 3DS challenge if re-submitting the transaction for authentication.
Use of Static Password		Visa does not permit the use of 3DS specific passwords except where Issuers need to use static password authentication to support diversity and disability inclusion.

Rule	Number ID#	Summary Description
Challenge screen data consistency	N/A	An Issuer must ensure that the 3DS Requestor Name and Transaction amount appear on the EMV 3DS challenge screen.
Use of Visa Secure technology	0029539	Visa Secure authentication technology must be used solely for the purpose of facilitating a Visa Transaction.
Issuer 3DS security requirements	N/A	An Issuer that does not operate its own ACS must use an approved ACS or DS supplier.
Biometrics Challenge Availability	N/A	Issuers must be able to support biometric authentication for EMV 3DS transactions. Fall-back options must also be available.
Minimum Data Requirements	N/A	Merchants must provide the required EMV 3DS data elements as defined in Appendix A.1.
Minimum Data Requirements	N/A	Merchants are also required to use the 3DS Method if the Method URL is provided by the Issuer.
Risk Based Authentication Capability	N/A	Issuers are required to support RBA for EMV 3DS and must evaluate the risk level of each transaction using some form of risk-model, rules engine, or risk analysis, and then apply the required authentication procedure.
Authentication Response Time Threshold	N/A	Issuers must provide response to the original EMV 3DS authentication request (AReq) within 5 seconds.
Abandonment Rate Threshold	N/A	Cardholder authentication abandonment rates for EMV 3DS transactions must not exceed 5%.
EMV 3DS Availability to Merchants	N/A	Effective 14 October 2020 Acquirers must ensure that all of their acquired e-commerce merchants have the ability to authenticate their e-commerce transactions through EMV 3DS version 2.2 or higher.
ECI 06 Quality of Service Program	0029326	Issuers must not systematically decline transactions submitted as attempted authentications (ECI 06).
Issuer Access Control Server (ACS) Availability	N/A	An Issuer's ACS must be available at least 99% of the time.



Rule	Number ID#	Summary Description
Authorization flagging and response support - Acquirer requirements	N/A	Acquirer must implement flags or appropriate data elements in the authorization system enabling their merchants to indicate to Issuers exemptions, Delegated Authentication and out of scope transactions for both PAN and token transactions.
Authorization flagging and response support	N/A	Acquirers must be able to receive the response code 1A (Additional customer authentication required) in Field 39 Response Code.
Authorization flagging - Issuer requirements	N/A	Issuers must be able to recognize flags submitted by Acquirers in the authorization system indicating exemptions, Delegated Authentication and out of scope transactions.
Authorization response - Issuer requirements	N/A	Issuers may only use a response code 1A (SCA required) for a transaction that is not permitted under regulation to be out of scope.
Issuer requirement to recognize MITs	N/A	Issuers must be able to recognize transactions that are MITs.
Authorization data accuracy – exemption handling	N/A	<p>If a merchant submits an authorization request that carries an SCA exemption, that exemption must be appropriate and reflect the correct nature of the exemption.</p> <p>Acquirers must have suitable controls in place to validate exemption flags submitted by their merchants, to ensure that the applicable flag is used for any given Transaction.</p>
Authorization data accuracy – out of scope handling	N/A	<p>A merchant can only submit a transaction indicated as an MIT if the cardholder agreement to process the MIT was set up either:</p> <ul style="list-style-type: none"> <li>• Prior to 14 September 2019; or</li> <li>• On or after 14 September 2019, providing SCA was applied on the mandate setup (with some specific exceptions).</li> </ul>
Authorization data accuracy – merchant name	N/A	The merchant name used in the 3DS authentication process should match the one used during the authorization process. This is to ensure that transactions may be dynamically linked, in accordance with regulation.
Indicating a transaction is an MIT	N/A	An Acquirer must have implemented flags or appropriate data elements in the authorization system enabling their merchants to indicate MIT transactions as out of scope of SCA.
Issuer requirement to Evaluate each Transaction	0029326	Issuers must be able to recognize exemptions and out of scope transactions and must not systematically decline or

Rule	Number ID#	Summary Description
		block authorization or token provisioning requests or transactions.
Issuer SCA requirement (1)	N/A	Issuers needing SCA to be performed by a merchant may decline authorizations with the response code 1A (SCA required).
Issuer SCA requirement (2)	N/A	Issuers may not decline transactions with a response code 1A (SCA required) if the authorization request includes a valid CAVV.
Use of decline codes – Issuer requirements	N/A	<p>An Issuer must ensure correct usage of SCA decline codes, specifically:</p> <ul style="list-style-type: none"> <li>• An Issuer must only use an SCA decline code where no other decline code is applicable.</li> <li>• An Issuer must not use an SCA decline code for transactions deemed out of scope from a regulatory perspective.</li> <li>• Issuers may only use an SCA decline code for these Transactions when they believe the Transaction has been incorrectly flagged /is not permitted under regulation to be out of scope</li> <li>• An Issuer must not use an SCA decline code for zero value authorization/account verification requests, OCTs and refund authorization requests.</li> </ul>
Use of Response Code 1A: Acquirer action	N/A	If an Issuer returns a response code 1A, the Acquirer must pass on that response to the merchant and ensure that the reason is clearly communicated.
Use of Response Code 1A: merchant response	N/A	<p>If a merchant receives a response code 1A in the authorization process, they must not submit the same transaction for authorization with an alternative exemption indicator.</p> <p>If an Acquirer / merchant receives a SCA decline code in the authorization request, the merchant must ask the Issuer for a 3DS challenge</p>
3DS decline rule for TRA	N/A	If an Issuer receives an authentication request via 3DS with a TRA Acquirer exemption indicator, they may not decline the same transaction at authorization with a SCA required decline code.
Minimum monthly approval rates	N/A	<p>Visa will monitor approval rates to ensure that acceptance is not unduly impacted and to avoid systematic declines.</p> <p>The percentage of Issuer SCA decline code must NOT exceed Issuer average monthly decline rate and must not exceed 50% of total declined ecommerce transactions.</p> <p>An Issuer must also meet specified monthly approval rates.</p>

Rule	Number ID#	Summary Description
CAVV processing, expiry & reuse.	N/A	Clients must comply with CAVV processing requirements.

### 3.5.2 Visa 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 is developing 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.

Issuers that are processing SCA Transactions through EMV 3DS must comply with the performance requirements included in the Visa Guide *PSD 2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements*.

## 3.6 Visa Trusted Listing



### 3.6.1 Introduction to Visa Trusted Listing

Visa is building a capability for consumers 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'd like to add this merchant to their Trusted List. Once SCA has been completed, the merchant will, subject to Issuer approval, be added to the customer's Trusted List. The customer can manage their Trusted List on their Issuer's web or mobile banking application. Subsequent visits to trusted merchants should generally not require SCA.

### 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 2.2.0 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 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 as a Trusted Beneficiary in their wallet page, when saving a card on file, or after the transaction completes. The merchant will send a request through EMV 3DS 2.2.0 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

Customers will be able to manage their Trusted List through their Issuer, either online or in their mobile app. The customer will be able to view the Trusted List and add or delete merchants from their Trusted List. The API that enables this is available from summer 2019. More details will be published when available. Customers will also be able to call the Issuer's customer service to remove a merchant from their Trusted List.

For more details please refer to 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

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:** Effective April 2019, 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 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 Note: Merchants may also participate in Visa Trusted Listing through the Visa Token Service. More information forthcoming
- **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 2.2.0. 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 2.2.0 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 Transaction Advisor



### 3.7.1 Introduction to Visa Transaction Advisor

Visa Transaction Advisor (VTA) is a Visa Solution that may assist clients to apply the TRA exemption available under PSD2. VTA will conduct a pre-authentication check and return values for whether the transaction qualifies for the Visa TRA program and a TRA score.

### 3.7.2 The Benefits of VTA

Visa Transaction Advisor provides an effective service for helping clients determine if a transaction qualifies for the PSD2 TRA exemption. This can deliver important benefits to both merchants, Acquirers and Issuers.

#### 3.7.2.1 Fraud Reduction

VTA uses advanced predictive analytics from millions of historical transactions to score numerous unique risk attributes submitted to VTA by clients. The score generated by VTA can provide additional insight to Issuers and Acquirers who can use the score to make more informed authorization decisions, with the aim of reducing fraud.

#### 3.7.2.2 Reduce Shopping Cart Abandonment

VTA is designed to reduce shopping cart abandonment by enabling merchants to apply SCA exemptions instead of requiring cardholders to provide SCA. The goal is higher approval rates, due to additional data for better decision making, with a more seamless experience for the cardholder.

### 3.7.3 How VTA Works

Clients connect to the VTA API through the Visa Developer Platform (VDP). VTA will combine data from the API call, historical data, and third party service provider data to return a risk score, determine if fraud thresholds have been exceeded and indicate whether both PSPs are within the EEA. Key API results are summarized below<sup>21</sup>:

- TRA Score
- EEA domestic indicator
- ETV amount exceeded indicator (500 EUR)
- RFR exceeded indicator for Acquirer and Issuer
- 180 day RFR exceeded indicator for Acquirer and Issuer
- Articles 2 & 18 low risk indicator

If an Acquirer decides to utilize the TRA exemption for a given transaction, they can submit an authorization request to Visa with the TRA exemption request indicator in Field 34. Information from the associated pre-authentication VTA API request will have been shared with a Visa data repository for linking with the authorization submitted by the Acquirer on behalf of the merchant or the merchant's payment facilitator. VisaNet will be able to reference this data repository during an authorization request using a unique key in the message and submit the VTA results to the Issuer to provide more data to inform the Issuer's authorization decision.

Visa's VTA service is based on the information available to Visa at the time of the transaction. It is the ultimate responsibility of the PSPs to ensure that any exemptions requested and accepted are valid per the regulation.

For more information please refer to the *Visa Transaction Advisor Implementation Guide* or contact your Visa representative.

---

<sup>21</sup> For a complete list of API results, please see the *Visa Transaction Advisor API Specification*.

## 3.8 Visa Delegated Authentication



### 3.8.1 Introduction to Visa Delegated Authentication

PSPs can outsource operational functions of payment services to a third party. The Visa Delegated Authentication Program facilitates the delegation of the authentication process, making it easier for members to delegate authentication to third parties that are eligible to participate in the Program.

### 3.8.2 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 today, including by being able to provide SCA, are able to continue to define a consistent consumer payment experience through this Program when SCA is required at their business, whilst maintaining the 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 is performed in line with the regulatory requirements and that fraud is strictly and consistently managed.

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

### 3.8.3 Components of the Program

There are four key components to Visa Delegated Authentication:

- 1. Rules and Liability Framework:** Effective April 2019, 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. Issuers should familiarize themselves with the Program, its alignment to their internal policies, and identify any steps they should take before the Program commences. An Issuer is free to choose to opt-out
- 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
- 3. Transaction Identification:** On a per transaction basis, the delegated entity will flag to the Issuer that SCA was performed through 3-D Secure or Visa Token Service
- 4. Program Compliance:** Participants must comply with a fraud rate for transactions that have participated within Visa Delegated Authentication

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*.

## 3.9 Visa Merchant Purchase Inquiry (VMPI)



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

The Visa Merchant Purchase Inquiry (VMPI) service provides an opportunity to avoid disputes that are marked as fraud simply because customers have problems recognizing transactions.

Such disputes can artificially increase a PSP's fraud count and impact adversely on the ability to apply the TRA exemption.

Visa experience has shown that a significant proportion of both disputes and transactions unnecessarily categorized as fraudulent can be avoided if additional data that helps a customer to validate a transaction can be provided to Issuers and customers prior to disputes being raised. Leading merchants using VMPI have seen reductions in disputes of up to 35% and reductions in transactions unnecessarily categorized as fraudulent of up to 30%.

Merchants benefit from improved user experiences if PSPs are able to apply the TRA exemption more widely. They can also benefit from a reduction in the direct cost of disputed transactions. Participation in VMPI may also help merchants wishing to participate in the Visa Trusted Listing Program or the Visa Delegated Authentication Program to reach and maintain the qualifying fraud rates for these Programs.

VMPI can also help reduce fraud rates regardless of which party actually holds the liability.

### 3.9.2 Introduction to the VMPI service

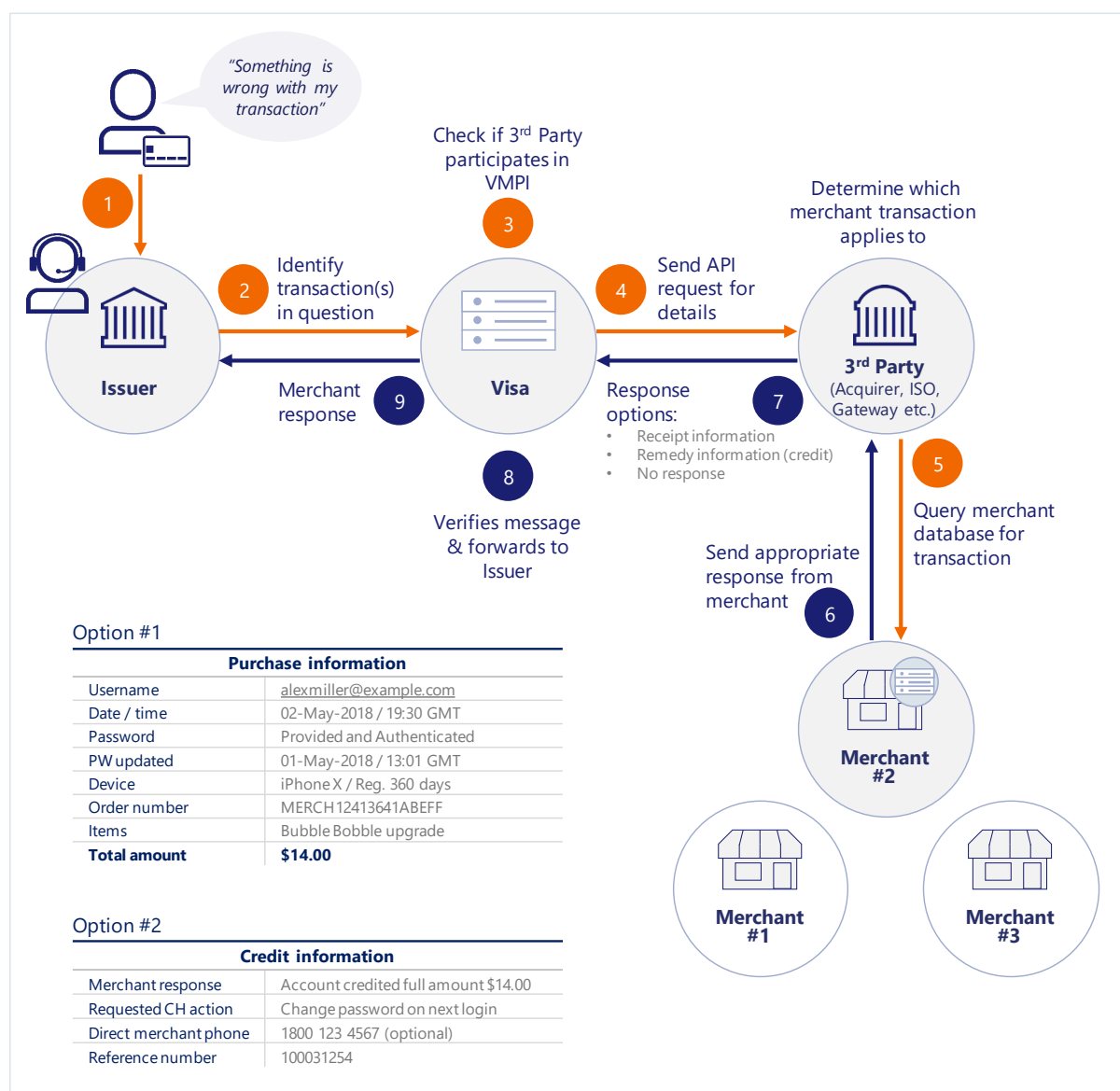
The VMPI service, which runs on Visa's dispute processing platform, connects merchants to Issuers prior to a dispute being submitted and fraud being reported. It is based around an API which allows additional transaction data to be presented to customers in real time.

VMPI also offers merchants the option of a notification of an intent to credit an account in near real time when a customer raises an inquiry. Such refunds, applied before disputes are raised, also help to reduce unnecessary disputes.

An overview of the VMPI process is shown in Fig 15 below:



**Figure 15: The VMPI process flow**



All European Visa Issuers are automatically enrolled in VMPI, are able to access the transaction information provided through the API and are required to use the data in the investigation stage of any dispute. In order to benefit directly, merchants need to enroll directly or via their Acquirer or payment facilitator.

### 3.9.3 Accessing VMPI

Merchants can access the service directly via the VMPI API through the Visa Developer Portal. Please note that in order to directly access the service, a merchant must be able to respond to requests with meaningful additional data within a 2.5 second response time. The data provided can be defined by the merchant based on its dispute resolution experience but may for example include SKU level information that will allow a customer to recognize a transaction.

Acquirers or third party processors can also participate and provide an on-behalf-of service by collecting the additional transaction data from their merchants. They can also offer the refund

service as an optional alternative which may be simpler if it is difficult to provide the data. Offering such a service can help to lower fraud rates across a PSP's portfolio.

Merchants, Acquirers and processors who are interested in VMPI should contact their Visa Account Executive. Merchants who are concerned that they may not be able to provide data within the target response time should contact their Acquirer or payment facilitator to see if they are able to offer an on-behalf-of service.

For more information on VMPI please visit the VMPI section of the Visa Developer Center at <https://developer.visa.com/capabilities/vmpi>.

### 3.10 The Visa MIT Framework



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

#### Best Practice

To avoid Issuers inappropriately declining transactions and requesting SCA even though the cardholder is not available, merchants must implement the MIT Framework.

The 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 MIT framework is not mandated to be used by merchants for PAN based transactions<sup>22</sup> (it is mandated for token based transactions). However, in the PSD2 context, if the framework is not used to identify transactions where the cardholder is not available to be authenticated, the Issuer will not be able to recognize the transaction 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.

The Visa MIT framework defines eight distinct types of MITs as summarized in Table 20 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 (ID) of the initial CIT<sup>23</sup>:** Located in Field 125, Usage 2, Dataset ID 03

For more details see Table 21 below.

<sup>22</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>23</sup> Or of the previous MIT in some cases as indicated in Table 20.

**Table 20: 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.</p> <p>This transaction type is based on an agreement with the cardholder and is not to be confused with cardholder initiated transactions performed with stored credentials (CITs are in scope of PSD2 whereas UCOF transactions are MITs and thus out of scope).</p>
Incremental	<p>An incremental authorization is typically found in hotel and car rental payment scenarios, where the cardholder has agreed to pay for any service incurred during the duration of the contract.</p>
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.</p>

**Table 21: 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>24</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

MITs will be considered as outside the scope of SCA requirements as long as the cardholder agreement to process the transaction was either:

- Set up prior to 14 September 2019<sup>25</sup>
- Set up on or after 14 September 2019, providing SCA was applied on the mandate setup if it was set up through a remote channel<sup>26</sup>

<sup>24</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.

<sup>25</sup> As noted in Section 2, NCAs may in some limited cases provide flexibility about their enforcement timescales. This may imply that MITs can be set up without SCA for a period after 14 September 2019, at the discretion of the local NCA. References to 14 September 2019 in this section should be read with this qualification.

<sup>26</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

It is the Acquirer's responsibility to ensure that any transactions they indicate as MITs meet one of the above requirements.

In addition to MITs that are 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 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 applies, even if the transaction may be subsequently completed via the use of an MIT.

- *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 applies, and the PSP considers there is no risk of fraud<sup>27</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.

---

fraud or other abuses. In Visa's view, SCA is required if the MIT mandate is set up via a face to face transaction – exemptions cannot be applied.

<sup>27</sup> For example use cases please Sections 5.11.1 and 5.17.

### 3.10.1 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 where the cardholder is not available 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.

#### 3.10.1.1 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.

#### 3.10.1.2 Grandfathering

For MITs covered by cardholder agreements that were established prior to 14 September 2019,<sup>28</sup> 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 14 September 2019 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.

- **Note:** Visa is aware that enhanced system development may be required to store transaction identifiers of previous transactions. Accordingly, to assist with merchant readiness in time for the PSD2 effective 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, Visa Acquirer-assigned interim transaction identifiers for use in place of a valid Original Transaction Identifier 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 transaction identifier<sup>29</sup>. Table 23 provides a view of the impact of using this Visa Acquirer-assigned interim transaction identifier.

<sup>28</sup> As noted in Section 2, local NCAs may in some limited cases provide flexibility about their enforcement timescales. This may imply that MITs can be set up without SCA for a period after 14 September 2019, at the discretion of the NCA. References to 14 September 2019 in this section should be read with this qualification.

<sup>29</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.

### 3.10.1.3 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 22.

- Note that for any of the transactions in Table 22, 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.4.

### 3.10.2 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 be authenticated during the transaction. Visa requires Issuers in the EEA to recognize MITs as out of scope of SCA requirements by 18 October 2019, but strongly recommends they are able to do so prior to the SCA effective date of 14 September 2019. They can do so using one of the following ways:

- The existing Visa MIT Framework, (see Table 21), or
- A New initiating party indicator introduced in Field 34 (see Table 22), 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 Response Code 1A (SCA required) 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.

#### 3.10.2.1 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 22. This enables Issuers to recognize a transaction as a MIT out of scope by simply looking for the value of “1” in that tag.



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 transaction identifier of the initial CIT (or previous MIT in some cases) in 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 transaction identifier of the initial CIT or of a previous MIT transaction. However, Visa has assigned transaction identifiers 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>30</sup>, indicating that the merchant/Acquirer was not ready to send a valid transaction identifier 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 transaction identifier of a valid initial CIT or previous MIT
    - This includes the transaction identifier 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 transaction identifier) starts to use a valid transaction identifier of a previous MIT.

Or:

- The interim Issuer transaction id of "0100000000000000"<sup>30</sup>
  - This is the case when a merchant was not ready to send a real transaction identifier 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 transaction identifier
- 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

<sup>30</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*.



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 22 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 22: 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)	Out of scope identifier Field 34 <sup>1</sup>	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125 <sup>2</sup> )			
Installment/ Prepayment	First Transaction (CIT) (May be of zero value if set up only)	I	--	--	Any valid <sup>3</sup> (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	I	--	Tran ID of first transaction/ previous MIT (or interim Tran ID)	10	1 <sup>1</sup>	N/A
Recurring	First Transaction (CIT) (May be of zero value if set up only)	R	--	--	Any valid <sup>3</sup> (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	R	--	Tran ID of first transaction/ previous MIT (or interim Tran ID)	10	1 <sup>1</sup>	N/A
Unscheduled Credential on File (UCOF)	First Transaction (CIT) (May be of zero value if set up only)	C	--	--	Any valid <sup>3</sup> (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	C	--	Tran ID of first transaction/	10	1 <sup>1</sup>	N/A

Description	Transaction Type	Visa MIT Framework			POS Entry Mode (PEM) (F22)	Out of scope identifier Field 34 <sup>1</sup>	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125 <sup>2</sup> )			
				previous MIT (or interim Tran ID)			
Incremental	First Transaction (CIT) (Estimated transaction) <sup>4</sup>	--	--	--	Any valid <sup>3</sup> (10 if stored credential)	--	Required
Incremental	Subsequent Transactions (MIT)	--	3900	Tran ID of first transaction	Any valid <sup>3</sup> (10 if stored credential)	1 <sup>1</sup>	N/A
Delayed Charges	First Transaction (CIT)	--	--	--	Any valid <sup>3</sup> (10 if stored credential)	--	Required
	Subsequent Transactions (MIT)	--	3902	Tran ID of first transaction (or interim Tran ID)	01 or 10 if stored credential	1 <sup>1</sup>	N/A
No Show	First Transaction (CIT)	--	--	--	Any valid <sup>3</sup> (10 if stored credential)	--	Required (except if secure corporate payment exemption applies)
	Subsequent Transactions (MIT)	--	3904	Tran ID of first transaction (or interim Tran ID)	01 or 10 if stored credential	1 <sup>1</sup>	N/A
Reauthorization	First Transaction (CIT)	--	--	--	Any valid <sup>3</sup> (10 if stored credential)	--	Exemption may be used

Description	Transaction Type	Visa MIT Framework			POS Entry Mode (PEM) (F22)	Out of scope identifier Field 34 <sup>1</sup>	Authentication
		POS environment (F126.13)	Message Reason Code (F63.3)	Original Transaction ID (F125 <sup>2</sup> )			
	Subsequent Transactions (MIT)	--	3903	Tran ID of first transaction (or interim Tran ID)	01 or 10 if stored credential	1 <sup>1</sup>	Not required but CAVV
Resubmission	First Transaction (CIT)	--	--	--	Any valid <sup>3</sup> (10 if stored credential)	--	Contactless exemption applies
	Subsequent Transactions (MIT)	--	3901	Tran ID of first transaction (or interim Tran ID)	01 or 10 if stored credential	1 <sup>1</sup>	N/A

Notes:

1. The new out of scope of SCA indicator 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.
2. 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 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, Transaction Identifier for each transaction, including subsequent MITs, in this field (except in the case of incremental authorizations where the initial transaction identifier is kept).
3. Any valid value because these transactions can also originate in F2F channels.
4. 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.
5. 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 23 for a visual representation of the impact of the usage of interim transaction identifiers in MITs, both from an Issuer and Acquirer perspective.

**Table 23: Acquirer and Issuer View of MIT Transactions with usage of Visa assigned interim transaction identifiers**

CIT Types	Visa Existing MIT Framework – Acquirer View <sup>31</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	Field 34, Tag 80 Dataset 02 <sup>32</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>33</sup>	-	3900	Tran ID of initial CIT	-	3900	Tran ID of initial CIT	1

### 3.11 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.

<sup>31</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>32</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>33</sup> An Acquirer assigned transaction identifier must not be used on incremental transactions

Visa provides a turnkey authenticator app for clients who are looking to launch a 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 center.

Visa also provides an SDK that clients who would like to integrate the biometric experience directly into their mobile applications. The SDK supports a device's built-in biometrics for example, proprietary fingerprint recognition, with other biometric authentication techniques such as facial & voice recognition.

The service allows clients to set their own risk based authentication policies by mixing and matching various biometric authentication factors against their user cases. For example, if the transaction is deemed to be of low risk then the customer can be asked to authenticate via their device's built in biometrics, if the transaction is of a higher risk then the customer can be asked to authenticate by using facial or voice recognition or both.

The SDK uses Fast Identity Online Alliance (FIDO)<sup>34</sup> security protocols. FIDO standards and is delivered through a specialist Visa partner.

More information is available via the Visa Developer Centre at <https://developer.visa.com/capabilities/biometrics>.

### 3.12 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 the ability to decide if and when additional authentication is needed. When SCA is required, VCAS supports multiple methods 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>.

---

<sup>34</sup> For more information visit: <https://fidoalliance.org>

# 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.

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 3DS and/or authorization request fields.

Visa is providing 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.

## 4.2 Key principles

### 4.2.1 The difference between Authentication and Authorization



The application of SCA and exemptions may be delivered through and impacts both the authentication and authorization 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 and, where required, takes place before authorization, using the Issuer's selected authentication method, which in most cases will be 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

These processes can be used to indicate the nature of the transaction, whether it is out of scope (indicated in authorization only), requires SCA, or is being processed under one of the exemptions. Transactions that are out of scope are most likely to be sent directly to authorization without authentication being deployed (although in some cases, such as one-leg-out transactions, the Issuer or Acquirer must still use best efforts to perform SCA). However, merchants and Acquirers do have a choice in how to indicate an Acquirer exemption to the Issuer. They may either:

- Submit transactions via 3DS for authentication with an exemption request flag and then submit to authorization with the appropriate authentication data including an exemption flag<sup>35</sup>
- Submit transactions direct to authorization with an exemption flag. If the Issuer accepts the exemption no further additional authentication is needed, however Acquirers should note that the Issuer has the right to request Resubmission via 3DS if it assesses that authentication is required.

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

### 4.2.2 Dynamic Linking



#### 4.2.2.1 Visa's interpretation of the regulation

The dynamic linking requirement (SCA RTS article 5) ensures that the customer is made aware of the transaction details (amount and payee) and authorizes the specific transaction matching those details. As such, the Issuer must be able to demonstrate that the cryptogram generated as part of the authentication process is specific to that transaction (including the amount and payee).

Visa's view is that this can be achieved by the sharing and validation of the CAVV or TAVV which gives cryptographic proof that the authentication completed successfully.

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 a mismatch.

---

<sup>35</sup> Available for Trusted Beneficiaries and TRA exemptions

Current Visa systems allow Issuers to check for exact matches between hashes of the merchant names submitted at authentication and authorization but do not allow for real-time analysis of variances, with fuzzy matching logic. This is due to space limitations in the CAVV that only support a hashed version of the merchant name, rather than the complete authentication merchant name. However, the information provided in the CAVV may be used to support reactive validation, for example in the case of a customer query or dispute.

Where differences do occur to the amount or 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, and where the amount is not known in advance, it must not exceed what the payer could reasonably have expected.

In the event that the system is compromised, there must be a mechanism in place to protect the cardholder.

#### 4.2.2.2 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
- 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.
- 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.

Table 24 summarizes the key characteristics of each Version:



**Table 24: CAVV Characteristics**

Characteristics Supported	CAVV Version 0	CAVV Version 1	CAVV Version 7
3DS Version	3DS 1.0 and EMV 3DS	3DS 1.0 only	3DS 1.0 and EMV 3DS
Merchant Name	No	No	Yes <sup>36</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*.

Issuers can use the CAVV to link to the authentication message, thus meeting the requirement. 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.

Issuers are strongly advised to not systematically decline transactions where there is not an exact match of merchant name or amount between the CAVV/TAVV and the authorization message as there will be valid instances where there is not an exact match. Furthermore, recent analysis of the data suggests a very low match rate between merchant names in the two flows - across all merchant use cases.

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

- Total transaction amount
- Merchant descriptor name<sup>37</sup> (where required)
- 3DS requestor ID

<sup>36</sup> A hashed version of the authentication merchant name is provided in version 7 of the cryptogram.

<sup>37</sup> For more information on populating the merchant name when the party requesting authentication is not the merchant that will request authorization see Section 4.6.2.8. 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*.



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.
- An MIT can only be submitted after a previous CIT (even if it is a zero-value transaction) has been performed to establish the initial agreement with the cardholder.
- Note that subscription type payments that are initiated by the payee only are processed in the Visa system as “recurring payments”. These are processed as MITs and considered by Visa to be out of scope.
- **A cardholder-initiated transaction (CIT)** is any transaction where the cardholder actively participates in the transaction. This can be either at a terminal in-store or through a checkout experience online. When the transaction is online or via a mobile application it can be facilitated either as a guest checkout, or with a stored payment credential that the cardholder has previously consented to store with the merchant.
- **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.4.

#### 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.



Irrespective of the business processes that a merchant uses for eCommerce transactions, there are some fundamental principles, which PSD2 and Visa have defined, 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 and in the addendum to this guide *Implementing Strong Customer Authentication (SCA) for Travel and Hospitality*.

#### 4.2.4.1 Out of Scope transactions

If a payment transaction is 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 3.2.8

#### 4.2.4.2 Visa principles for implementing SCA

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

The following Table 25 summarizes Visa's guiding principles for implementing SCA in common payment use cases for both CIT and MIT transactions.

**Table 25: 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 differs by more than a cardholder reasonably expects <sup>38</sup>
	Establish agreement for ongoing/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>39</sup>

<sup>38</sup> What is within the reasonable expectations will depend on the circumstances and the transparency to the cardholder. If not within the reasonable expectations of the cardholder, SCA would be required. This represents Visa's view of what is acceptable based upon the opinion of the EBA. Merchants should check the position of individual National Competent Authorities with regard to allowing variations in final amounts with reasonable customer expectations.

<sup>39</sup> This does not apply in some specific cases outlined in Section 3.10 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).

Transaction Type	Use Cases	Recommendation for SCA?
Merchant Initiated	Executes payment (e.g. subscriptions, No Show)	Out of scope. SCA is required in most cases when the initial mandate 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

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

The following Table 26 summarizes Visa's guiding principles for implementing SCA in common non-payment use cases.

**Table 26: 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.

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

Table 27 summarizes key principles that should be applied to the authentication and authorization and clearing processes.

**Table 27: Fundamental Visa authentication, authorization and clearing principles for implementing SCA**

Principle	Rationale
Visa Authentication Principles	
<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; 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 a response code 1A (SCA required). 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 2.1.0 and it will be an integral feature within EMV 3DS 2.2.0. This enables merchants to obtain authentication data (CAVV, ECI) in the absence of the cardholder for transactions previously authenticated.</p> <p>The feature can be used to enable merchants to effectively manage some complex 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> <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>

Principle	Rationale
	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.).
<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 currently qualify the merchant for liability protection under the Visa Rules. More information will be provided by the Visa Token Service as these new options become available.
<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.
Visa Authorization Principles	
<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>40</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>
<b>8. MITs must be properly indicated as MITs to ensure they are treated as out of scope of SCA</b>	<p>If a merchant initiates an electronic transaction based on a prior agreement with a customer, the transaction is out of scope of SCA as long as Issuers can indeed 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</p>

<sup>40</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
	therefore out of scope of PSD2 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.
<b>9. Merchants need to store the Transaction ID of the CIT (or of a previous MIT for 3 of the MIT types) that established the agreement for future MITs.</b>	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.
<b>10. Merchants should only request authorization when the goods are available and ready to be shipped</b>	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.
<b>11. Authorizations are valid for a maximum of up to 7 days</b>	If an authorization cannot be fully cleared after 7 calendar days <sup>41</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.
<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>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 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</p>

<sup>41</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>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 or 06) 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 or 06) 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 a response code 1A (SCA required)<sup>42</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) 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</p>

<sup>42</sup> A merchant should not submit a CAVV older than one year as the CAVV will fail validation.



Principle	Rationale
	<p>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.</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>43</sup>.</p>
<p><b>14. Transaction amounts can vary between authentication, authorization and clearing within “reasonable” customer expectations<sup>44</sup></b></p>	<p>It is for the PSPs involved to ensure compliance with PSD2. However, as a matter of Visa’s requirements, the final transaction amount authorized can vary from the amount authenticated as long as it remains within the customer’s reasonable expectations. The amount of the authorization should not be higher than the amount the cardholder can reasonably expect based on the circumstances and amount presented to the cardholder at time of authentication.</p> <p><b>As an outside limit,</b> Visa requires that the authorized amount must never exceed the amount authenticated by more than 15%. Any authorization amount that is greater than this is not subject to Visa’s 3-D Secure 2.0 Program chargeback protection and may be charged back by the Issuer. (Refer to <i>Merchant/Acquirer Implementation Guide for Visa’s 3-D Secure 2.0 Program; Visa Supplemental Requirements</i>, for more information).</p> <p>It is best practice that when the final transaction amount is not known in advance, that a merchant / Acquirer should authenticate the customer for the estimated maximum transaction amount. In this situation, to avoid abandonment due to confusion, it is essential to clearly communicate to the customer before the authentication step that:</p> <ul style="list-style-type: none"> <li>• They are authenticated for a maximum amount</li> <li>• They will only be charged for what they purchase (which may be lower than the authenticated amount)</li> <li>• No charges will appear on their card statement until the order is finalized</li> </ul> <p>• It is also considered best practice that if the previously communicated maximum amount is exceeded, then customer re-authentication for a new amount should be sought immediately.</p>

<sup>43</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).

<sup>44</sup> Principle 14 is Visa’s view of what is allowable based upon the opinion of the EBA. Merchants should check the position of individual National Competent Authorities with regard to allowing variations in final amounts with reasonable customer expectations.

Principle	Rationale
	<ul style="list-style-type: none"> <li>• <b>The final amount cleared can vary from the amount authorized as long as it remains within the customer's reasonable expectations.</b> The amount cleared should not be higher than the amount the cardholder can reasonably expect based on the circumstances and amount presented to the cardholder at time of authentication. <ul style="list-style-type: none"> <li>• <b>As an outside limit,</b> Visa requires that the cleared amount must never exceed the amount authorized by more than 15%. The exact percentage varies for some MCCs. For more information please refer to Visa Rule ID# 0025596.</li> </ul> </li> <li>• <b>The final transaction amount cleared can be lower than the amount authorized.</b> Visa Rules allow for the cleared amount to be lower than the amount authenticated and authorized. If the authentication provides the merchant with fraud liability protection, the protection still applies despite the variance.</li> <li>• <b>The authenticated amount, the authorized amount and the cleared amount can be different.</b> There are many legitimate reasons why the amount authenticated, amount authorized and amount cleared could be different. This is acceptable provided the variance is within the customer's reasonable expectations and the other limits defined above.</li> </ul> <p>Where the final amount is not known when the cardholder authenticates the transaction, the authentication code should be specific to the amount the cardholder agreed to be blocked (e.g. the 'maximum amount').</p>
<b>15. Issuers must not respond to the authorization request for out of scope transactions with a response code of 1A (SCA required)</b>	An Issuer must not use a response code 1A (SCA required) 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 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.
<b>16. Grandfathering can be applied to MITs performed based on agreements made prior to 14 September 2019<sup>45</sup></b>	A merchant with an existing agreement with a customer established prior to 14 September 2019 does not need to establish a new agreement with their customer with SCA. Instead, all MIT authorizations performed after the 14

<sup>45</sup> As noted in Section 2, NCAs may in some limited cases provide flexibility about their enforcement timescales. This may imply that MITs can be set up without SCA for a period after 14 September 2019, at the discretion of the relevant NCA. References to 14 September 2019 in this section should be read with this qualification.

Principle	Rationale
	<p>September 2019 can reference either the "initial" CIT, or the transaction ID of any previous related transaction processed before the 14 September 2019 (CIT or MIT). This is subject to any arrangement with local CAs, which may provide flexibility to establish a new MIT arrangement without SCA for a limited period after 14 September 2019. 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 14 September 2019.</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 14 September 2019.</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 /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> </ul> </li> <li>• No amount should be authenticated or authorized in the case where an agreement includes an allowance for conditional future charges using 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.</li> </ul>

Principle	Rationale
	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.
Visa Clearing Principles	
<b>18. Multiple clearing records can be submitted for a single authorization</b>	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 <sup>46</sup> . Because a CAVV is not included in clearing, submitting multiple clearing records to fulfil a single authorization does not impact merchant fraud liability.

#### 4.2.5 Who can apply exemptions?



Under the regulation, the application of exemptions is restricted to regulated PSPs (in the case of card payments Issuers and Acquirers) however there is scope for merchants to work with their Acquirers to set and execute exemption policies.

Table 28 below summarizes which PSP is able to apply which relevant exemption for remote card transactions according to the regulation.

**Table 28: Summary of who may apply an exemption<sup>47</sup>**

Exemption	Issuer	Acquirer
Trusted beneficiaries	Yes	No <sup>1</sup>
Transaction Risk Analysis (TRA)	Yes	Yes <sup>2</sup>
Low Value Transactions	Yes	Yes <sup>2,3</sup>
Secure corporate payment processes & protocols	Yes	N/A

Notes:

- Under the PSD2 regulation, an Acquirer may not apply the trusted beneficiaries exemption, however EMV 3DS 2.2.0 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

<sup>46</sup> For more information on how to handle multiple clearing records for a single transaction, refer to Visa Rules ID#0027756 and ID#0028914

<sup>47</sup> Adapted from Table 2 in the EBA Opinion Paper on the Implementation of the RTS on SCA and CSC 13 June 2018

- 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.
2. 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.
  3. 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.

Note that Visa does not provide any indicator for the recurring transactions exemption as the exemption does not apply to Visa cards; 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.

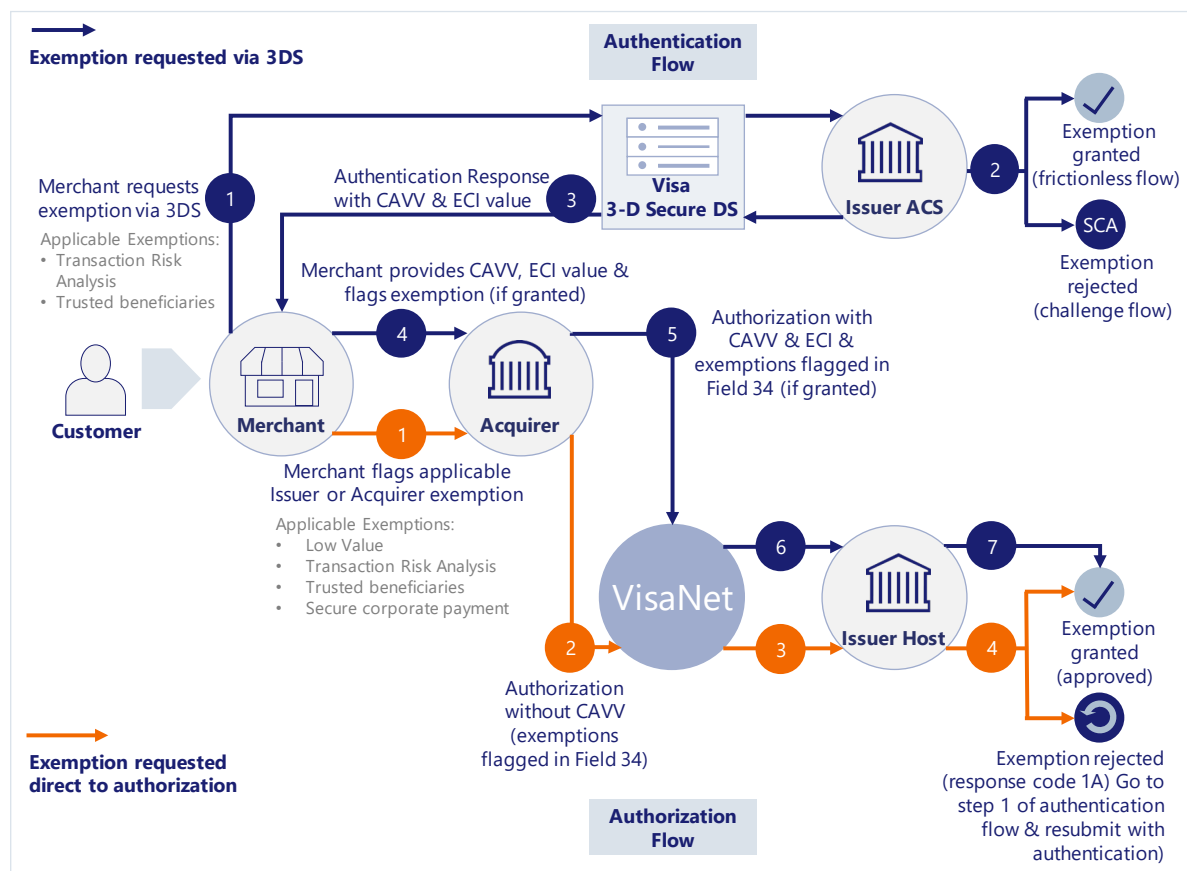
#### 4.2.6 Options for merchants & Acquirers regarding exemption application



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 3DS 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 3DS message first, before performing an authorization request. This is done by setting the relevant indicators in the 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 step-up, even if authorization will be delayed. Merchants should be aware that if taking this approach, the exemptions exercised during authentication 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, there are specific types of exemptions that are only available in the authorization (but not in the authentication). However, merchants considering this option should be aware that the Issuer can decline the exemption and request an authentication. 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.
- **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 managing the authentication flow



Strategies to optimize the application of SCA and exemptions in a PSD2 environment will be driven by decisions that merchants, Acquirers and Issuers need to take at key points in the transaction process flow.

This section summarizes these flows and decision points from the perspective of:

1. The merchant/Acquirer
2. The Issuer

At each decision point is a description of the options available to the merchant/Acquirer and the factors that should be taken into account when deciding how to treat the transaction from the perspective of applying SCA or an exemption. This is done for:

1. A Standard Customer Initiated E-Commerce Transaction
2. Setting up an MIT agreement
3. A Merchant Initiated Transaction

Detailed differences and options that arise with other common and complex use cases are covered in section 5. More detailed practical guidance on the application of exemptions is given in section 4.5.

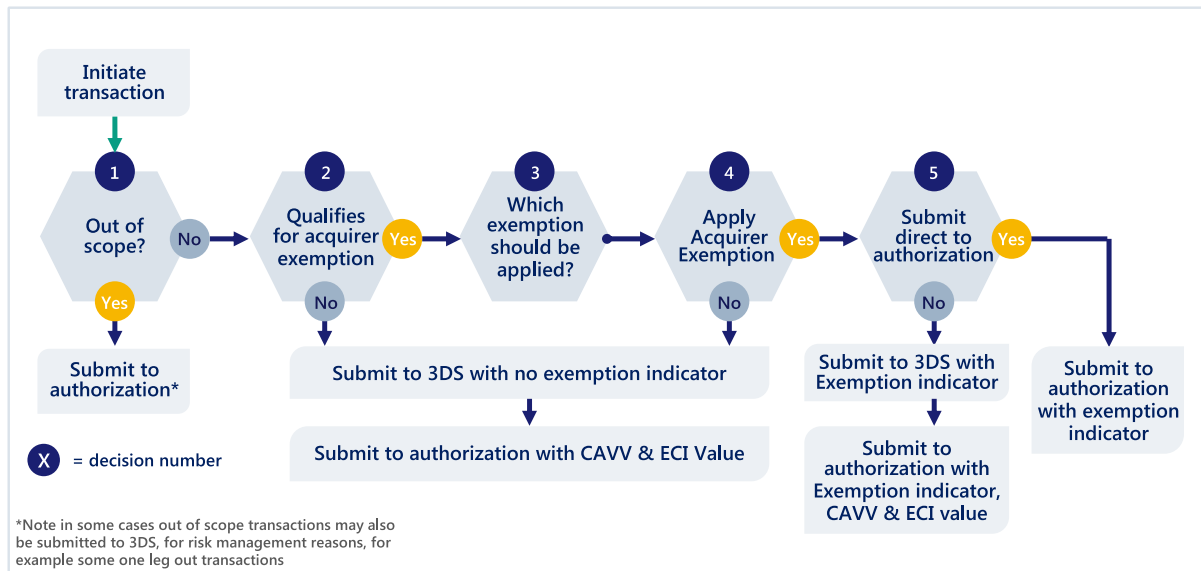
Note, these flows are based on the example where the merchant uses 3DS for authentication. If an alternative authentication method is used, for example under the Visa Delegated Authentication Program) then variations may apply. More information will be made available during 2019.

### 4.3.1 Merchants/Acquirer Decision Flow

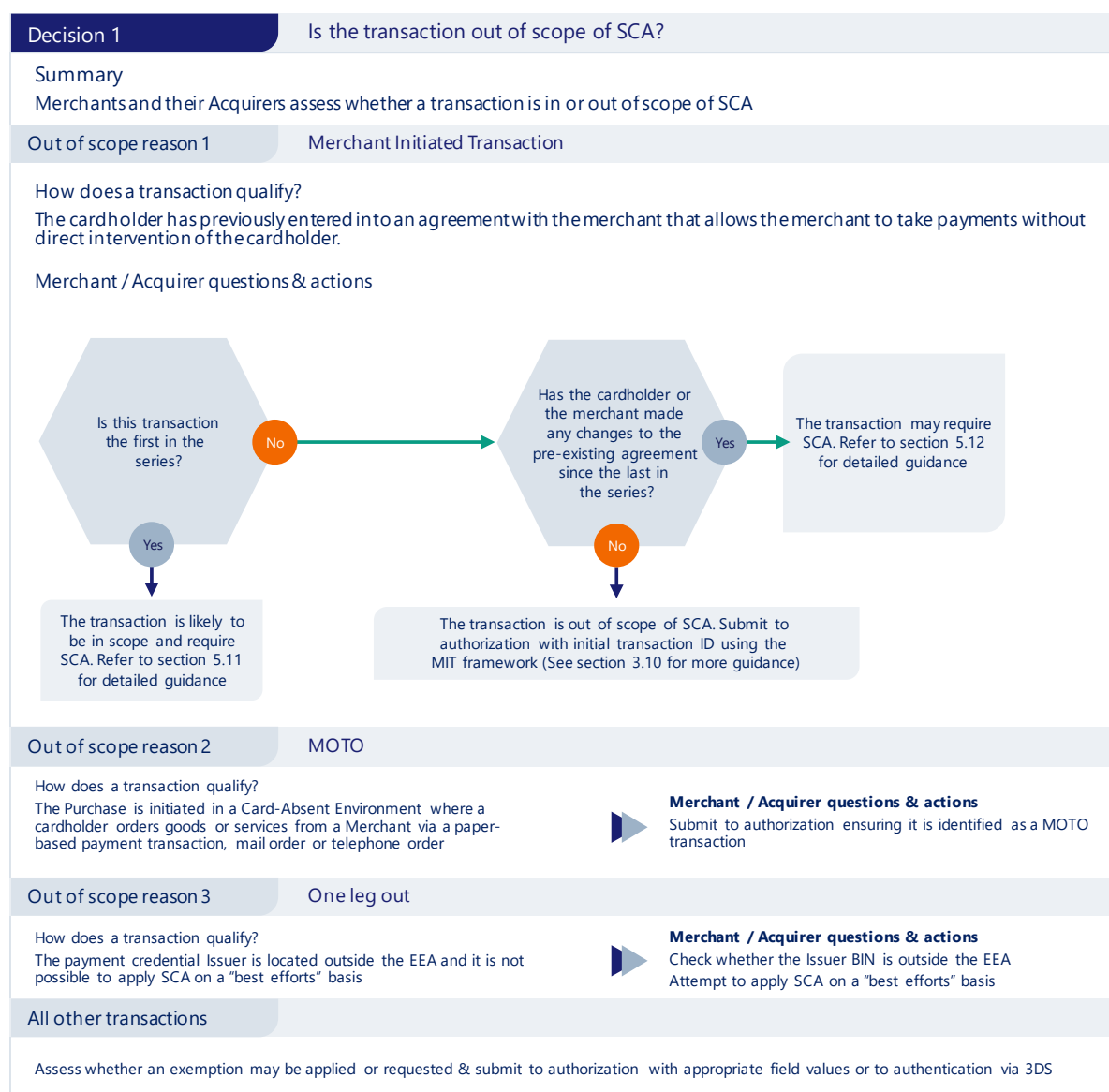


Figure 17 summarizes the key decision points for the merchant/Acquirer. Figure 18 provides more detailed guidance on the options and decision criteria at each decision point.

**Figure 17: The key decision points in the merchant/Acquirer flow**



**Figure 18 Merchant/Acquirer SCA/exemption simplified process flows and decision points**





## Decision 2

## Does the transaction qualify for an Acquirer exemption?

### Summary

Assessment of whether there is an option for the Acquirer to apply 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.

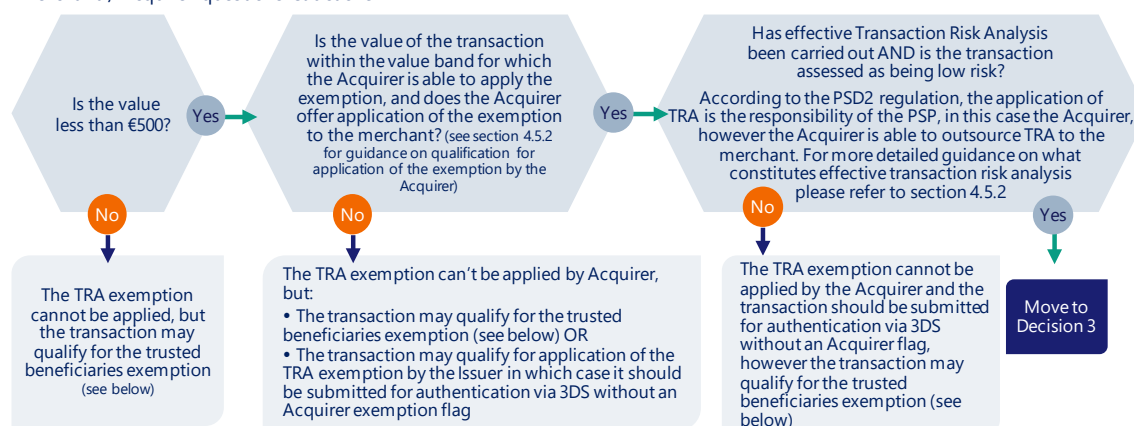
### Exemption 1

#### 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 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*

While the PSD2 regulation allows for the Acquirer to apply this exemption, in reality only the Issuer will know whether the transaction qualifies under the velocity limits. Acquirers should apply the TRA exemption to low value transactions.

### 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 3.10

### Exemption 4

#### Trusted Beneficiaries Exemption

How does a transaction qualify?

- Merchant is qualified for application of the trusted beneficiary, *and*:
- The cardholder has added the merchant to its list of trusted beneficiaries that is held and managed only by the Issuer (existing trusted beneficiary)

Is the merchant enrolled in the Visa Trusted Listing Program or otherwise approved by the Issuer to qualify for the trusted beneficiaries exemption?

If yes, move to decision 3.

If no, Trusted beneficiaries exemption cannot be applied. Submit the transaction for authentication via 3DS without an exemption flag

### Exemption 5

#### Secure Corporate Payments Exemption

How does a transaction qualify?

- The transaction is undertaken using a commercial virtual card or lodged card, *or*:
- A physical commercial card issued to an individual is used within a secure corporate payment process or protocol approved by the local Competent Authority

If a virtual card or lodge card is used, this will be recognised and the exemption applied by the Issuer.

If a physical commercial card is used within a secure payment process or protocol, the Acquirer can request application of the exemption using the secure corporate payments indicator in field 34.

### Decision 3

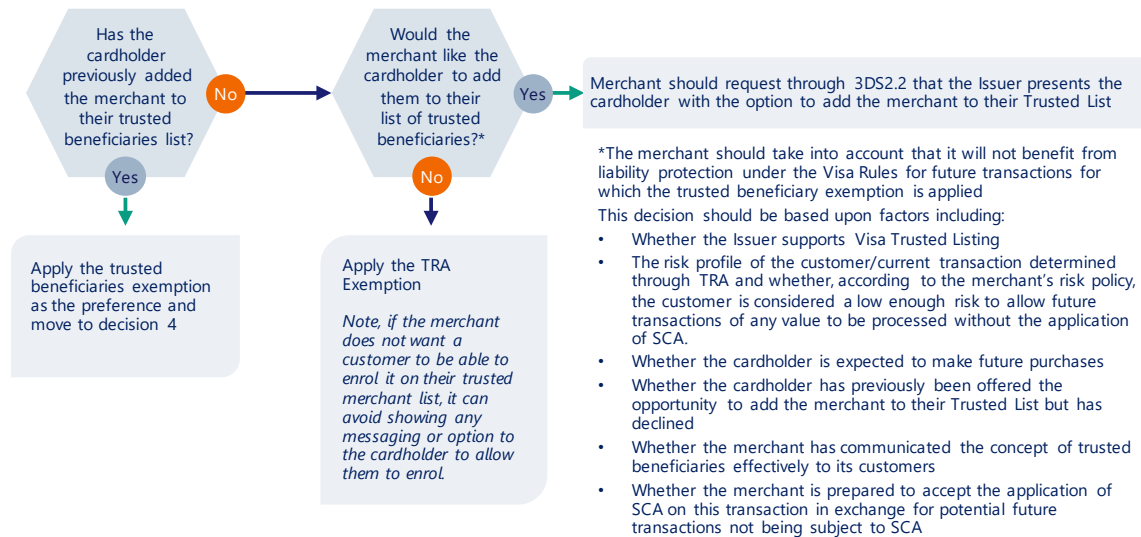
### Which applicable exemption should take priority?

#### Summary

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 Exemption

### Summary

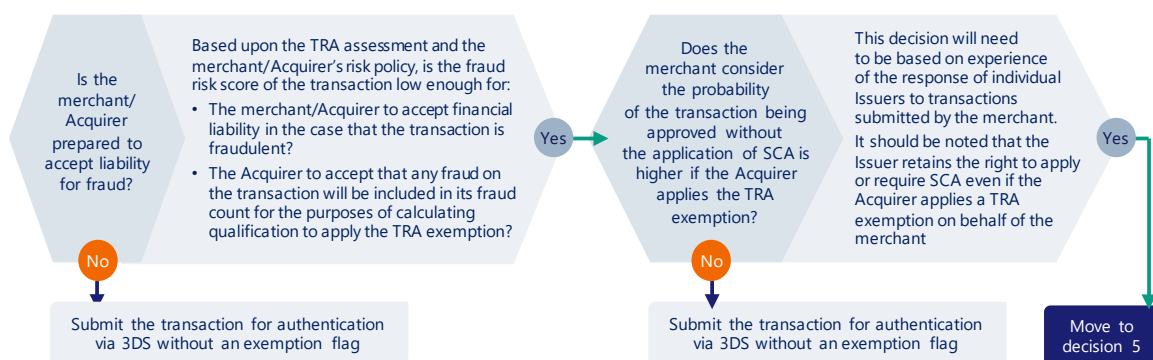
Should an allowable exemption be applied by the Acquirer or requested by the merchant?

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 in the case of TRA or at all in the case of trusted beneficiaries
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

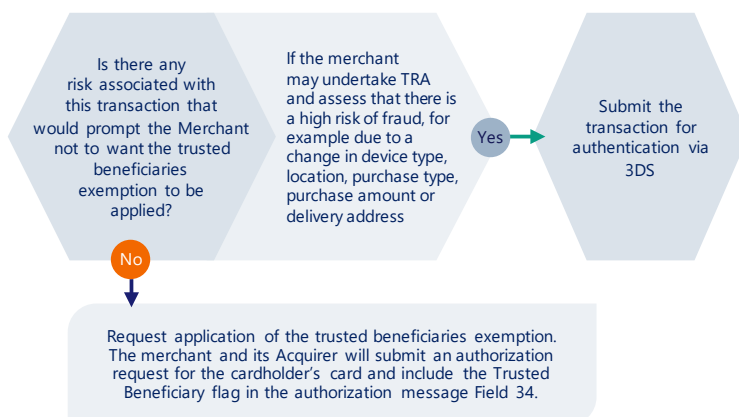
### Transaction Risk Analysis



### Trusted Beneficiary: Merchant already added to the cardholder's Trusted List

Note, the default position is that if the cardholder 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

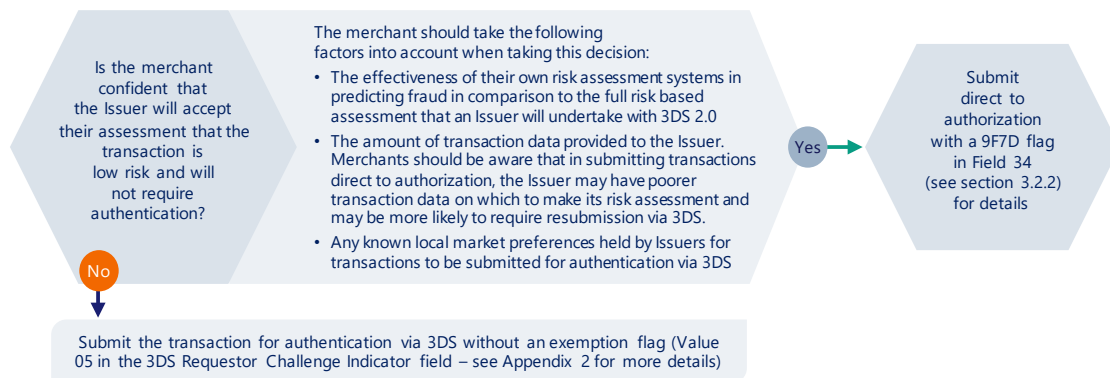
A merchant submitting a transaction with an Acquirer exemption applied has the option to either submit via 3DS or direct to authorization with appropriate flags set (see section 3.2.2 for details)

The decision will be based on the merchant's assessment of the balance between the following factors:

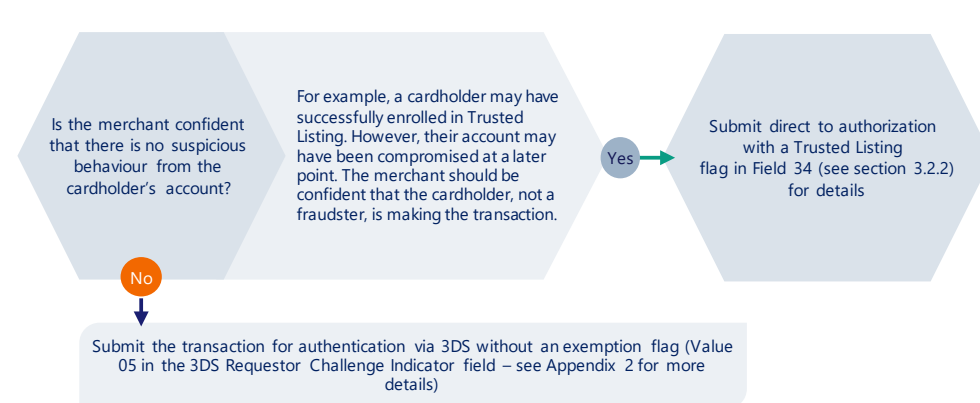
- The merchant's own level of confidence in their assessment of the risk of the transaction
- A balanced evaluation of the risk that any challenge may present to the cardholder abandoning the transaction. Whilst this should not be an issue with 3DS 2.0, any friction in the purchase always carries a risk no matter how small that something might disrupt the purchase
- In consideration of the above, a merchant must also evaluate 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 to be applied
- Know local market preferences held by Issuers for transactions to be submitted for authentication via 3DS
- 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.*

### Transaction Risk Analysis



### Trusted Beneficiary



#### 4.3.1.1 Additional Considerations for merchants and Acquirers considering sending transactions straight to authorization

If a merchant/Acquirer sends a transaction straight to authorization and the Issuer's risk assessment determines it high risk, it may issue a response code 1A requesting that the transaction is resubmitted for the application of SCA, for example via 3DS. Merchants and Acquirers should 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 a response code 1A 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 flag in the authorization request if they are submitting transactions under an Acquirer exemption. Transactions without exemption flags or without having had SCA applied are likely to receive a response code 1A (SCA required) from the Issuer, as the Issuer will not know that the exemption is being requested and thus will not have an audit trail in the data.

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

#### 4.3.1.2 Acquirer Policy Decisions

Acquirers will need to develop policies on risk assessing transactions that are sent straight to authorization with or without exemption fields set. These should aim to minimize the unnecessary application of response code 1A (SCA required) while staying in line with the Issuers risk management policy.

##### Key Point

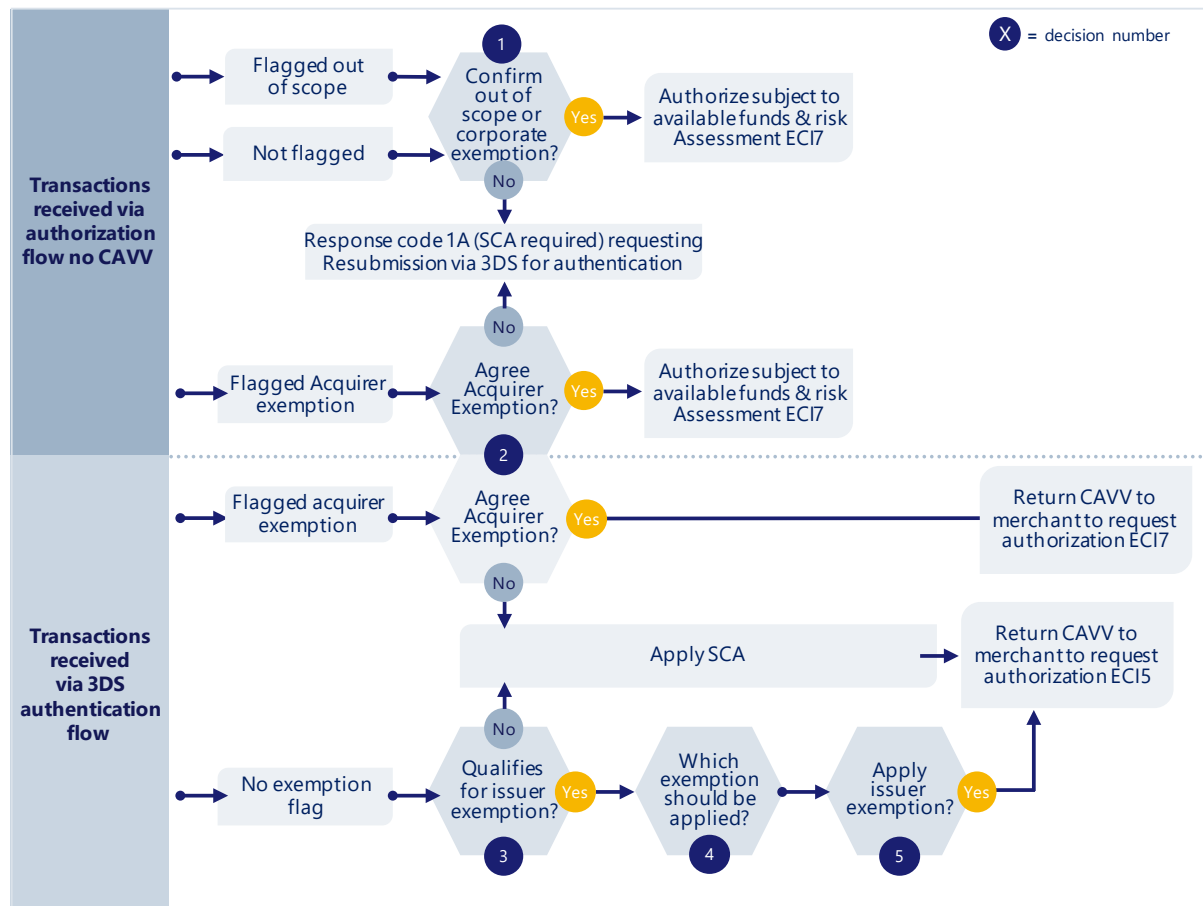
Acquirers must also ensure they pass any response code 1A (SCA required) on to their merchants rather than aggregating them with other generic decline codes such as "Do Not Honour" so merchants have visibility of the nature of decline and are able to respond to this particular message to re-submit the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

Acquirers should develop policies on the risk profile of transactions that may be sent straight to authorization with exemption flags set in order to provide merchants that qualify with the opportunity to take advantage of the facility while minimizing the risk of fraud and response code 1A (SCA required).



Issuers may receive transactions either direct to authorization or via 3DS. The Key Decision points in the Issuer flow for both sets of transactions is summarized in Figure 19 below. The detailed options and decision considerations at each decision point are detailed in the subsequent Figure 20:

**Figure 19: Key Issuer decision points**



**Figure 20: Issuer key decision flow**

Decision 1		Confirm the Transaction is out of scope of or does not otherwise require SCA
<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.		
Out of scope reason 1	Merchant Initiated Transaction	
How does a transaction qualify? The transaction is received with an appropriate indicator	▶	<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 local competent authority). 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 3.10.2 for more information on identification of MITs Authorize, subject to normal authorization assessment criteria (availability of funds etc) The Issuer must not issue a response code 1A (SCA required) due to lack of authentication
Out of scope reason 2	MOTO	
How does a transaction qualify? The transaction is received with an appropriate indicator	▶	<b>Issuer actions</b> Authorize, subject to normal authorization assessment criteria (availability of funds etc). Do not decline or issue a response code 1A (SCA required) due to lack of authentication
Out of scope reason 3	Anonymous payment	
How does a transaction qualify? The payment credential is not directly linked to an individual consumer (for example an anonymous prepaid gift card)	▶	<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 a response code 1A (SCA required) due to lack of authentication
Out of scope reason 4	One-Leg-Out	
How does a transaction qualify? The Acquirer is outside the EEA.	▶	<b>Issuer actions</b> Authorize, subject to normal authorization assessment criteria (availability of funds etc). Do not decline or issue a response code 1A (SCA required) 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
Other Transactions not requiring SCA		
How does a transaction qualify? OCTs, refunds & some zero value authorization/verification requests	▶	<b>Issuer actions</b> Check for indicators described in section 3.2.8 and zero value transaction scenarios described in 4.6.2.2. Do not decline or issue a response code 1A (SCA required) due to lack of authentication
Unflagged Transactions		
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.	▶	<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 a response code 1A (SCA required) due to lack of authentication

## Decision 2

## Does the Issuer agree with the Acquirer 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 process, 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.

Issuer 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 3DS 2.0 with an appropriate exemption indicator (requires support of version 2.2 of the 3DS spec)

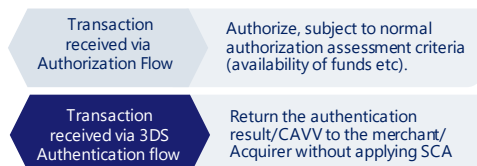
Issuer options and actions:

#### 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
- The Acquirer will assume liability for fraud count in the context of qualification to apply the exemption against reference fraud rates

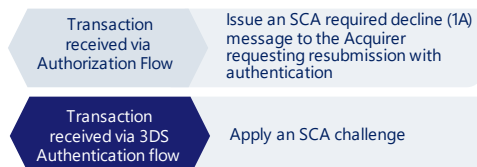
Note: some local competent authorities may require that any fraud is taken into account in the fraud counts of both Acquirer and Issuer regardless of which party applies the exemption



#### 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?

- Merchant is qualified for application of the trusted beneficiary exemption by the Issuer, and
- The cardholder has added the merchant to its list of trusted beneficiaries that is held and managed only by the Issuer (existing trusted beneficiary)



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 an individual is used within a secure corporate payment process or protocol approved by the local Competent Authority

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 required decline (1A), 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

Recurring transactions

Trusted beneficiaries

Secure corporate payments

Note: Guidance on the application of the Secure Corporate Payments Exemption is under development and will be included in a later version of the guide.

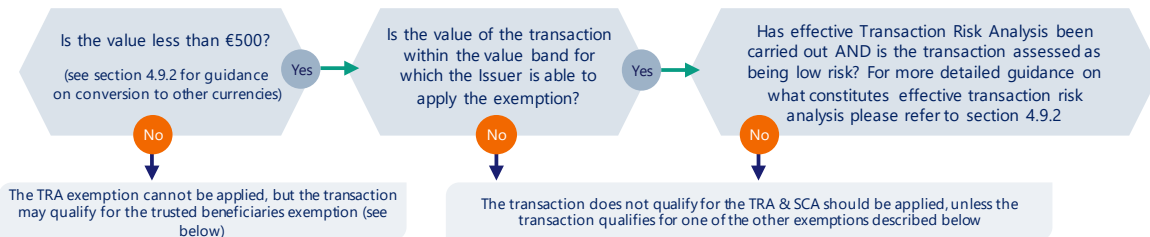
### Exemption 1

### 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

Merchant / Acquirer 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 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 zero value transactions and velocity counters should not be incremented for zero value transactions. Zero value transactions do not require the application of SCA.

### Exemption 3

### Recurring transactions

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

Issuer options and actions

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 4

### Trusted beneficiaries

How does a transaction qualify?

- The merchant is qualified for application of the trusted beneficiary exemption by the Issuer, and
- The cardholder has added the merchant to its list of trusted beneficiaries that is held and managed only by the Issuer (existing trusted beneficiary)

Issuer options and actions

So long as the Issuer determines that the qualifying criteria apply, the Issuer may apply the trusted beneficiaries exemption.

#### Decision 4

#### Which applicable exemption should take priority?

##### Summary

Assuming the transaction could qualify for either the trusted beneficiaries, or low value, or TRA exemption, which exemption should take precedence?

*Note only one exemption should be applied*

The decision on which exemption should take precedence when the transaction qualifies for more than one will depend upon factors including:

- Liability protection
- The benefits of the additional data shared under a TRA exemption applied through 3DS

#### 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**

#### 4.3.2.1 Issuer Policy Decisions

Issuers need to develop policies on risk assessing transactions that are sent straight to authorization with or without exemption fields set. These should aim to minimize the unnecessary application of response code 1A (SCA required) while staying in line with the Issuers risk management policy.

### 4.4 Liability for fraud-related chargeback

Table 29 below summarizes how liabilities for fraud-related chargeback apply between the Issuer and the Acquirer under the Visa Rules depending on which PSP applies an exemption and whether the transaction is submitted via 3DS<sup>48</sup>. Exemptions applied by the Acquirer must have an exemption flag in F34 in the authorization request to be considered valid by the Issuer.

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 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 flag, 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.

<sup>48</sup> PSD2 sets out its own principles of liability as a matter of regulation, but does not preclude PSPs from making additional arrangements.

**Table 29: Use of 3DS and Application of Liabilities for Common Transaction Use Cases**

SCA Provision		PSP Applying Exemption	Submitted Via 3DS	Challenge Applied	Fraud Liability under Visa Rules
Exemption	Transaction Risk Analysis (TRA)	Issuer	Yes	No	Issuer ECI 05
		Acquirer	Yes	No	Acquirer ECI 07
		Acquirer	Yes	Yes	Issuer ECI 05
		Acquirer	No	N/A	Acquirer ECI 07
	Trusted Beneficiaries	Issuer	Yes	No	Acquirer ECI 07
	Low Value	Issuer	Yes <sup>49</sup>	No	Issuer ECI 05
		Acquirer	No <sup>50</sup>	N/A	Acquirer ECI 07
	Corporate processes and protocols	Issuer	Yes	No	Issuer ECI 05
		Issuer	No	N/A	Acquirer ECI 07
		Acquirer	No	N/A	Acquirer ECI 07
Out of Scope	Merchant Initiated Transaction (MIT)	N/A	Yes (initial transaction)	Yes	Issuer ECI 05
			No (subsequent transaction)	No	Acquirer ECI 07
			Yes (transaction using the Reauthorization indicator that carries a CAVV and associated ECI 05)	Yes (however exemption may be applicable)	Issuer ECI 05
	Anonymous cards	N/A	Yes	No	Acquirer ECI <sup>51</sup>
		N/A	No	No	Acquirer ECI 7
	MOTO	N/A	No	No	Acquirer ECI blank, 1, or 4
	One-leg-out	N/A	Yes	Optional	Issuer ECI 05
		N/A	No	N/A	Acquirer ECI 07

<sup>49</sup> Note Issuers will only be able to apply the low value exemption in 3DS if they are able to synchronise the counters with authorization and therefore it may be more practicable for the Issuer to apply the TRA exemption.

<sup>50</sup> An Acquirer may only request the application of the low value exemption using the appropriate indicator in Field 34 of the Authorization request (as there is no low value exemption indicator in 3DS) but has no visibility of the counter and therefore takes the risk that the counter has been exceeded.

<sup>51</sup> This is for the scenario when the anonymous card is not enrolled in 3DS. If the card was enrolled in 3DS (some maybe) then the Issuer could authenticate and provide an ECI 05.

SCA Provision		PSP Applying Exemption	Submitted Via 3DS	Challenge Applied	Fraud Liability under Visa Rules
SCA Required	Does not qualify for an exemption or transaction is a CIT setting up or changing an MIT series agreement when such a change requires SCA	N/A	Yes	Yes	Issuer 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.

### 4.5.1 The low value exemption



The difficulties in deploying the low value exemption have been described in section 4.3. While this may prove to be a useful exemption to apply for payments that do not warrant the application of complex risk and authentication technology, payments should also not be considered low risk just because they are of low value. Issuers need to ensure:

- They have velocity checking against the cumulative low value transaction count or amount limits in place and that the Issuer's ACS is linked to the velocity checking in the Issuer's host system.
- The host is able to increment and reset the velocity counters correctly based when a Low Value exemption and/or RBA and is applied.
- 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 required decline (1A) should the maximum value or transaction count be exceeded.

Issuers should note that:

- The Issuer host can keep track of transactions that have had authentication applied by checking the authentication method value in Field 126.20<sup>52</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

<sup>52</sup> See Section 3.2.5 for more detail on Field 126.20 and the list of authentication method indicator values

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.

- The cumulative transaction count should not be incremented for zero value transactions that do not require SCA. See Section 4.6.4.2 for more information on these transactions.

## 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.

Recital 14 of the RTS states that: “risk-based requirements should combine the scores of the risk analysis, confirming that no abnormal spending or behavioral pattern of the payer has been identified, taking into account other risk factors including information on the location of the payer and of the payee with monetary thresholds based on fraud rates calculated for remote payments”.

Article 2 of the RTS also states that: “Payment service providers shall ensure that the transaction monitoring mechanisms take into account, at a minimum, each of the following risk-based factors: (a) lists of compromised or stolen authentication elements; (b) the amount of each payment transaction; (c) known fraud scenarios in the provision of payment services; (d) signs of malware infection in any sessions of the authentication procedure; (e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.”

Visa requirements for the deployment of Risk Based Analysis 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 Appendix A.1. 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.

### 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.<sup>53</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 30: 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 ecommerce transaction rates and consumers switching to alternative, lower friction payment methods or Issuers.
  - Breaching the Visa rule limiting transaction abandonment (see section 3.5 for more details).

---

<sup>53</sup> (Reference: EBA: Opinion Paper on the implementation of the RTS on SCA and CSC - June 2018, para 47).

#### 4.5.2.5 Calculation of fraud rates

The PSD2 regulation<sup>54</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.
- 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 once they go over the reference fraud rates.

Visa's view is that in the case that one of the PSPs (the Issuer or the Acquirer) applies the TRA exemption, any fraud from that transaction should only be attributable to the fraud count of the PSP that applied or requested the exemption, but PSPs need to be responsible for determining their own fraud rates in accordance with the legal requirements of PSD2.

### 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 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
- 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.

---

<sup>54</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.

- The customer may add or remove the merchant to or from their Trusted List, through an Issuer controlled experience
- 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 transaction. 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,

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>55</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.

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 VTL



The Visa Trusted Listing Program provides a complete hosted solution for Issuers minimizing the development and operational overhead associated with offering a trusted beneficiaries solution. For more details on the Visa Trusted Listing Program, please refer to Section 3.6 and the *Visa Trusted Listing Implementation Guide*.

<sup>55</sup> See Visa Rules ID #0030633. For more details refer to the *Visa Trusted Listing Program Implementation Guide*



#### 4.5.3.4.1 Customer Experience



##### 4.5.3.4.1.1 3-D Secure:

Visa will support PAN or token enrollment through EMV 3DS 2.2.0 or VTS. The cardholder, who is eligible to participate, can add a merchant in two ways:

1. During a transaction, a customer can be prompted to list their card through the ACS screens of 3-D Secure. Once the customer opts in and performs strong customer authentication, then the merchant is saved to the customer's Trusted List and the transaction completes.
2. A customer can be prompted to add a merchant to their list, outside of a purchase flow (e.g. when saving a card on file with a merchant) to opt in and add the merchant to their list and perform strong customer authentication through 3-D Secure.

The Trusted Listing enrollment through token provisioning is expected to be available late 2019.

##### 4.5.3.4.1.2 Authorization

Once the customer has listed a merchant, subsequent transactions should not require additional authentication. The Acquirer can send the transaction through authorization, with the Trusted Listing exemption flag in Field 34 and the VMID in Field 126.5. The transaction will flow to Visa, where Visa will validate the status of the PAN and VMID to determine if the relationship is still in an active list.

Visa will support both PAN and token in the authorization flow.

#### 4.5.3.4.2 Liability



##### 4.5.3.4.2.1 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 authentication under the Visa Trusted Listing Program.

##### 4.5.3.4.2.2 Disputes

If a merchant and its Acquirer participate in Visa Trusted Listing and choose to send the trusted beneficiaries exemption flag, 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. This is only the case where the payments are initiated electronically through dedicated payment processes or protocols that are not available to consumers.

PSPs must ensure that, and NCAs must be satisfied that, those processes or protocols guarantee at least equivalent levels of security to those provided for by PSD2. NCAs may have their own procedures or processes for authorizing use of this exemption and Visa recommends that Issuers liaise with NCAs 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 Corporate, not consumer products

The exemption may only be applied where the payer using the dedicated payment processes or protocols is an incorporated entity, such as a company or a public sector organization. The exemption may not be applied where the payer is a consumer or, if a consumer card is used within a secure corporate payment process.

###### 4.5.4.2.2 Corporate products to which the exemption may be applied

Visa considers that lodged or virtual commercial cards such as those used within an access-controlled corporate travel management or corporate purchasing system, would potentially be within scope of the exemption.

These products are defined as follows:

- **Lodged card:** A card account that is issued to a corporate customer (a company or organization), not an individual, and is typically held by or "lodged" with a procurement entity such as a Travel Management Company (TMC) approved by the corporate customer to make authorized purchases or bookings on behalf of the corporate customer. No physical card is issued. The lodged card allows purchases to be initiated on behalf of the corporate customer while the payment transaction takes place directly between the corporate customer and the supplier of the goods or services being provided.
- **Commercial virtual card:** Typically, a single use or limited multi-use card number with an expiry date and security code, that is issued to a designated and authorized user acting on behalf of a corporate purchaser for a business to business transaction initiated through a secure electronic purchasing system. The virtual card number will typically have other restrictions applied to it such as a maximum transaction value that corresponds to the purchase amount and will be limited to use with a single defined merchant or merchant category. No physical card is issued. Virtual cards are typically used where it is efficient for a merchant to receive B2B payments via individual card transactions rather than bulk invoicing and settlement. An example is travel agencies settling booking payments with hotels.

Visa also considers that physical commercial cards issued to employees for business expenditure when used within an access-controlled corporate travel management or

corporate purchasing system, could also be within scope of the exemption. An example would be where the credentials associated with a physical commercial payment card that has been issued to a named employee are held within a corporate Travel Management Company (TMC) profile and used by that TMC to purchase corporate travel services booked by the TMC on the employee's behalf.

However, 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. This means that Issuers will need to ensure that physical commercial cards are enrolled in 3DS to enable SCA to be applied when required.

Similarly, physical consumer cards, were they to be used within a secure payment process (for example lodged with a TMC) would not qualify for the exemption. In this case, SCA would need to be applied, otherwise the PSP would be in breach of its legal obligations under PSD2 and the Issuer would decline the transaction at authorization. Corporate customers and procurement providers such as TMCs may wish to consider policies to prevent personal cards from being used for purchases that they arrange.

#### 4.5.4.3 Examples of a secure dedicated payment process or protocol?

In addition to lodged cards and virtual cards described above, the use of physical commercial cards, issued to a named employee cardholder may, subject to the view of local regulators, be considered secure payment processes or protocols when used in secure corporate environments such as:

- Corporate Travel Management Companies (TMCs) that store commercial card details of client employees with a secure profile that are only accessible by authorized employees through a secure log-in process
- Corporate travel booking tools 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

#### 4.5.4.4 Who is responsible for the secure payment process or protocol and application of the exemption?

The regulation places a requirement on PSPs to:

- Provide NCAs with 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 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

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

For practical guidance on the application of the exemption for Issuers and merchants and on the use of the Secure Corporate Payment Indicator please refer Section 5.15.

## 4.6 Additional Guidelines for Issuers

### 4.6.1 Issuer selection and deployment of EMV 3DS challenge methods - ensuring security with a seamless UX



Providing both secure and consumer friendly challenge methods are vital to ensure all cardholders in an Issuer's portfolio are able to complete an SCA challenge with minimal abandonment. Visa currently intends to introduce minimum abandonment rate thresholds from October 2019 which require Issuers to ensure abandonment rates are below 5%. How easy it is for consumers to transact online will be a key factor in their decision to keep a card top of wallet.

#### 4.6.1.1 Factors driving selection of challenge methods

Issuers need to develop strategies for adoption of challenge methods that achieve an appropriate balance between the following considerations:

- Compliance with the SCA factor requirements of PSD2 as summarized in Section 2.1
- Simplicity of user experience and minimization of friction when a challenge is required
- Effective support of app and browser-based checkouts
- Compliance with Visa Rules on abandonment and latency (see Section 3.5)
- Social inclusion
- Security of challenge methods and resistance to exploitation by fraudsters
- Availability/reliability
- Cost

#### 4.6.1.2 The development of inclusive strategies

3-D secure supports multiple SCA challenge options, many of which are delivered via a smartphone or standard mobile handset. It is expected that most Issuers will offer options to customers to ensure that they are able to complete SCA challenges independently of device ownership, mobile network coverage and physical disability.

Visa proposes an SCA Authentication Factor Strategy that provides staged compliance and consumer choice by providing two primary authentication methods:

- Biometric plus device possession
- SMS OTP plus Risk Based Authentication

Visa's view is that biometric based challenges delivered via pre-registered, trusted smart phones will deliver the best balance between compliance, security and minimization of UX friction in the medium term. Visa is implementing a rule that will require Issuers to support biometric solutions. However, it is recognized that not all customers will own a biometric capable device or wish to use biometric challenge methods.

Visa is also enhancing 3DS to incorporate behavioral biometrics into the data provided through 3DS. This will enable a compliant SCA solution using an OTP as evidence of possession and the behavioral biometric as evidence of inherence.

In addition, Issuers should offer an accessibility option for use in limited circumstances for customers who are unable to access mobile device based authentication methods. The main authentication options are summarized in Table 31.

**Table 31: Potential SCA Challenge Options**

Challenge Method	Description	Advantages	Disadvantages
Native device Biometric	<p>Built in phone biometric (for example fingerprint) is used to provide inherence factor and prove possession of device.</p> <p>In the case of fraud, the merchant is liable if outside 3DS, the Issuer is liable if the biometric is used as a 3DS challenge</p>	<ul style="list-style-type: none"> <li>• Seamless user experience</li> <li>• Consistent biometric experience for all authentication experiences provides familiarity for customer</li> <li>• Does not require mobile network coverage</li> </ul>	<ul style="list-style-type: none"> <li>• Requires delegated authentication agreement with handset platform vendor</li> <li>• Issuer is reliant on a third party</li> </ul>
App based biometric	Facial, voice or behavioral biometric enabled by a banking or dedicated app	<ul style="list-style-type: none"> <li>• Seamless user experience</li> <li>• Handset does not require biometric sensor</li> <li>• Issuer controls authentication</li> <li>• Does not require mobile network coverage</li> </ul>	<ul style="list-style-type: none"> <li>• Requires stand-alone app</li> <li>• Inconsistent authentication experiences between services from different providers</li> </ul>
SMS OTP	OTP is delivered via SMS to validate device possession. <sup>56</sup>	<ul style="list-style-type: none"> <li>• Inclusive – most customers can access SMS</li> <li>• Already widely deployed</li> <li>• Works in conjunction with browser and app checkouts on various devices</li> </ul>	<ul style="list-style-type: none"> <li>• OTP can only be used to prove possession</li> <li>• Static card details are not a compliant knowledge factor</li> <li>• Visa does not recommend use with a static password due to adverse security and user experience implications</li> <li>• Security vulnerabilities</li> </ul>

<sup>56</sup> Note SMS OTP is used alongside a second independent factor, which is typically currently card data but in future should be inherence evidenced through behavioural biometrics

Challenge Method	Description	Advantages	Disadvantages
			<ul style="list-style-type: none"> <li>• Uncertainty over whether SMS OTP is acceptable to some local regulators</li> <li>• Requires mobile network coverage</li> <li>• Message cost</li> <li>• UX not as integrated as other options</li> </ul>
Out of Band App delivered OTP	As SMS, but OTP is delivered via a banking or other mobile app	<ul style="list-style-type: none"> <li>• More secure than SMS OTP</li> <li>• Does not require mobile network coverage</li> </ul>	<ul style="list-style-type: none"> <li>• As above – e.g. cannot be used with static card details as a compliant knowledge factor</li> <li>• Requires smartphone and use of app</li> <li>• Requires user to manually open out of band app (EMV 3DS 2.1.0 &amp; 2.2)</li> </ul>
OTP generator token	Standalone OTP generator device	<ul style="list-style-type: none"> <li>• Allows those without a mobile phone to authenticate</li> <li>• Does not require any connectivity</li> </ul>	<ul style="list-style-type: none"> <li>• Consumer needs to carry device</li> <li>• UX is more complex than alternatives</li> <li>• Cost of device distribution</li> </ul>

#### 4.6.1.3 Populating the 3DS challenge window

The challenge window needs to include the merchant name and amount and clearly show the card payment details. The challenge window should only include the request for the authentication factor that the customer is being asked to provide.

Additional 3DS UX guidelines for Issuers are available on the Visa Developer Centre.

#### 4.6.1.4 Considerations for Implementing Out-Of-Band Biometrics on 3-D Secure 2.1 and 2.2

3-D Secure 2.1 and 2.2 allows for Out-Of-Band (OOB) authentication, which increases the authentication options for users. OOB Authentication is defined by EMVCo<sup>57</sup> as:

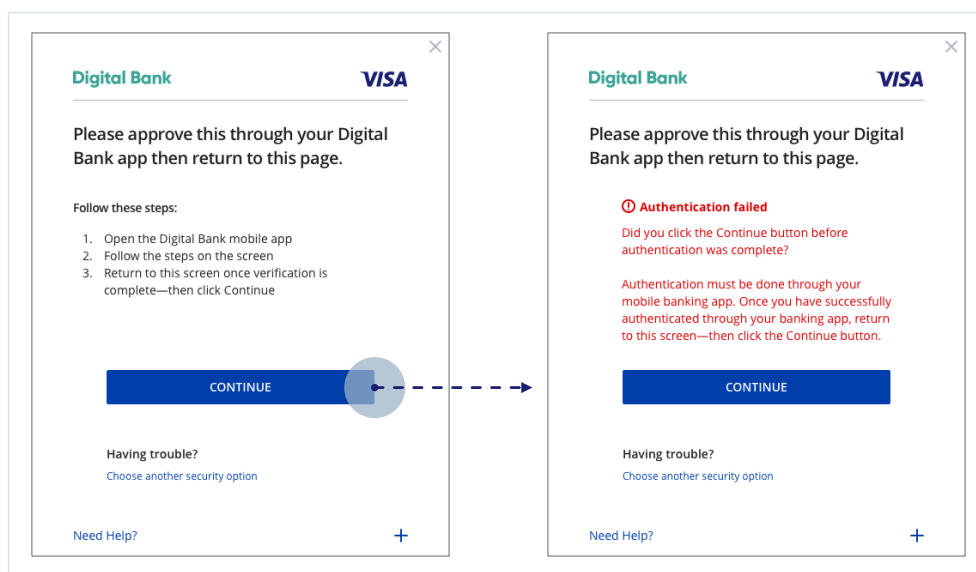
*A Challenge activity that is completed outside of, but in parallel to, the 3-D Secure flow. The final Challenge Request is not used to carry the data to be checked by the ACS but signals only that the authentication has been completed.*

<sup>57</sup> EMVCo. "EMV® 3-D Secure Protocol and Core Functions Specification" Version 2.2.0. <https://www.emvco.com/emv-technologies/3d-secure/>

Visa strongly recommends that Issuers and ACS providers wishing to implement OOB authentication only do so if they support EMV 3DS 2.2.0. The OOB user experience delivered by EMV 3DS 2.1.0 is confusing to customers and is likely to result in a high level of customer abandonment due to customer confusion. The reason for this is that in the EMV 3DS 2.1.0 user experience flow:

- The customer is required to carefully read the instructions presented in the secure checkout page of the merchant app or website
- The customer needs to manually open their mobile banking app to authenticate
- The secure checkout prompt includes a prominent “Continue” button that customers should only select once they have successfully completed the authentication through the separate online banking app. The presentation of this button is such that customers are very likely to select it before completing authentication, resulting in an error. The error message screen also contains a “Continue” button that should only be selected once authentication is completed. Again, the presentation of the button is such that customers are likely to select it before completing the authentication resulting in repeated error messages and likely transaction abandonment. The User experience is illustrated in Figure 21 below:
- EMV 3DS 2.1.0 does not support automatic return to the merchant’s secure mobile web or app checkout, again potentially resulting in transaction abandonment.

**Figure 21 Clicking ‘Continue’ before authentication is complete will result in an error**



In order to provide an optimized user experience, through both EMV 3DS 2.1.0 and EMV 3DS 2.2.0, Issuers and ACS providers need to keep several additional considerations in mind. These are summarized in Appendix A.3.

#### 4.6.2 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 for more information.

### 4.6.3 3RI authentication requests



Issuers supporting EMV 3DS 2.1.0 and above may receive 3RI requests for a new CAVV for a transaction under some of the scenarios defined in Section 5, such as delayed or split shipments. Each request for an updated CAVV should be assessed on its merits. Issuers must not blanket decline 3RI requests.

### 4.6.4 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 eCommerce.

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

#### 4.6.4.1 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 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 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 or issue a Response Code 1A (SCA required).

#### 4.6.4.2 Zero-value authorizations

There are a number of reasons why a merchant may perform a zero value authorization (Account Number Verification transaction) as documented in Section 5 and summarized in Table 32 below. It is important that Issuers understand this is the case and adopt appropriate processing policies as several zero-value transactions do not require SCA. In cases where SCA is required, the Issuer should rely on the merchant to request and provide the associated CAVV. If a zero-value transaction has no CAVV, no exemption indicator and is not of a type that is out of scope of PSD2, it does not require SCA and may not be declined with a response code 1A (SCA required). The only exception is use case #3 in Table 32 below, when SCA is required. Note that token-based zero-value authorizations that are not identified as MITs will continue to be submitted with a TAVV<sup>58</sup> even if the CAVV is not present.

---

<sup>58</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.



Zero-value 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.

**Table 32: Examples of zero value transactions and expected Issuer processing policy**

#	Conditions	Use cases represented and expected Issuer processing policy
1	<ul style="list-style-type: none"> <li>Zero value</li> <li>TAVV (if token)</li> <li>No POS environment (F126.13)</li> <li>No message reason code (F63.3)</li> <li>No initial Transaction ID (F125)</li> <li>No MIT indicator in Field 34, Tag 80 Dataset 02</li> </ul>	<p>This data represents three different scenarios:</p> <ul style="list-style-type: none"> <li>A standard Account Verification (refer to further description below) – in this scenario SCA is not required and therefore Issuers must not issue a response code 1A (SCA required) if no is CAVV present.</li> <li>Setting up an agreement for No Show, delayed charges and incremental (refer to further description below) – in this scenario SCA is required (CAVV must be present).</li> <li>Setting up an agreement for a delayed authorization (MIT reauthorization) – in this scenario SCA may be performed but an exemption may also apply. 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 Visa Rules<sup>59</sup>.</li> </ul> <p>As an Issuer will not be able to tell which of these three use cases a transaction is for, it has to rely on the Acquirer to provide a CAVV if SCA is required. If a CAVV is not present in the authorization request, the Issuer has to assume it is a standard account verification and should not decline requesting SCA.</p>
2	<ul style="list-style-type: none"> <li>Zero value</li> <li>TAVV (if token)</li> <li><b>'C' in POS environment (F126.13)</b></li> <li>No message reason code (F63.3)</li> <li>No initial Transaction ID (F125)</li> <li>No MIT indicator in Field 34, Tag 80 Dataset 02</li> </ul>	<p>This data represents two different scenarios</p> <ul style="list-style-type: none"> <li>Storing credentials on file for the first time for future CITs (refer Section 4.6.4.2.2 for more information). In this scenario SCA is required if there is a risk of fraud. In the eventuality that there is no risk of fraud, the CAVV is not</li> </ul>

<sup>59</sup> For more information please refer to section 4.2.4.3 Table 27 Principle 2.

#	Conditions	Use cases represented and expected Issuer processing policy
		<p>present and Issuers must not issue a response code 1A (SCA required).</p> <ul style="list-style-type: none"> <li>Note that future CITs performed with the credential will require SCA, or a suitable exemption.</li> <li>Setting up an agreement for a future Unscheduled Credential on file MIT (refer to further description below for setting up a subscription agreement) - in this scenario SCA is required (CAVV must be present).</li> </ul> <p>As an Issuer will not be able to tell which of these two use cases a transaction is for, it has to rely on the Acquirer to provide a CAVV if SCA is required. If a CAVV is not present in the authorization request, the Issuer should not decline requesting SCA.</p>
3	<ul style="list-style-type: none"> <li>Zero value</li> <li>TAVV (if token)</li> <li><b>'R' or 'I' in POS environment (F126.13)</b></li> <li>No message reason code (F63.3)</li> <li>No initial Transaction ID (F125)</li> <li>No MIT indicator in Field 34, Tag 80 Dataset 02</li> </ul>	<p>This data represents the scenario of Setting up an agreement for a subscription (recurring payment) or installment/ prepayment agreement (refer to Section 4.6.4.2.3 for more information) - in this scenario SCA is required (CAVV must be present).</p> <p>If the CAVV is not present or valid, then the Issuer must decline with response code 1A.</p>

#### 4.6.4.2.1 Standard Account Number Verification

An Account Number Verification is a zero-value transaction with:

- No value in Field 126.13 or in Field 63.3
- No CAVV
- TAVV (if token)
- No initial Transaction ID in Field 125

This is not a financial transaction, but a transaction processed purely to check the validity of a card. It is out of scope of PSD2 and Issuers should ensure it is not declined based on the lack of authentication. The merchant will check validity and will likely be doing a financial authorization including authentication data or suitable exemption flags later.

#### 4.6.4.2.2 Setting up a Stored Credential

A merchant may use a zero-value transaction when storing credentials for future CIT transactions and no payment is due at the same time. The zero value transaction will have:

- The value 'C' in Field 126.13
- No message reason code in Field 63.3
- CAVV (present in most cases, but could be absent in some)

- TAVV (if token)
- No initial Transaction ID in Field 125

SCA is required if there is a risk of fraud, which is likely in this case as card details are being provided. 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.

#### 4.6.4.2.3 Setting up an agreement for subscription and installment/prepayment or Unscheduled Credential MITs

A merchant may use a zero-value transaction to establish an agreement for future MITs if no initial charge is made at the time the agreement is made. SCA is required when the initial mandate is set up (see Section 5.11). Therefore, the zero-value transaction will have:

- An indicator in Field 126.13- R (for future recurring payment), C (for future unscheduled credential on file payments) or I (for future installment/prepayments), (and no value in Field 63.3)
- A CAVV and associated ECI value to prove authentication was performed
- A TAVV (if token)
- No exemption indicator in F34
- No initial Transaction ID in Field 125

This is a transaction to establish a mandate for future Standing instruction MITs, such as recurring payments (R), installments/prepayments (I) or Unscheduled Credential-on-File (C) – these are subscriptions at non regular intervals (not to be confused with CITs performed with stored credentials) and SCA is required.

Note that when the value C is used to indicate the setting up of an Unscheduled Credential on File MIT, the transaction will look like a transaction when setting up a stored credential where SCA “may” not have been performed. (See section 4.6.4.2.2).

#### 4.6.4.2.4 Setting up an agreement for Industry Specific MITs (No Show, Delayed Charges, Incremental and Reauthorization)

A merchant may use a zero-value transaction to establish an agreement for future MITs if no initial charge is due at the time the agreement is made. Where the initial mandate is set up via a remote electronic channel, SCA is required in most cases (see Section 5.11). Therefore, the zero-value transaction will have:

- No value in Field 126.13 nor in Field 63.3
- A CAVV to prove authentication was performed
- A TAVV (if token)
- No initial Transaction ID in Field 125

This is a transaction to establish a mandate to perform a future industry specific MIT, such as No Show, Delayed Charges Incremental or Reauthorization (used for delayed authorizations or split shipments). As there is no specific indicator to enable an Issuer to differentiate this zero-value transaction from a standard account verification, the Issuer should not decline the zero-value transaction on the basis that authentication is present or not in an account verification message. However, any future MITs using Message Reason Codes for No Show,

Delayed Charges, Incremental or Reauthorization must refer to the initial CIT where authentication was performed<sup>60</sup>.

#### 4.6.4.3 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).

#### 4.6.4.4 Reauthorizations

A number of the scenarios in Section 5 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>61</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 a zero-value 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

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 a response code 1A (SCA required), 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.

---

<sup>60</sup> Except if the secure corporate payments exemption was used when setting up the No Show agreement.

<sup>61</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.

#### 4.6.4.4.1 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.

#### 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.

#### 4.6.4.5 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>62</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 generally 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 (response code 1A, SCA required), as the cardholder is generally 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 3.10.2.

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

<sup>62</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*

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.

#### 4.6.4.6 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.

#### 4.6.4.7 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".

#### 4.6.4.8 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.

#### 4.6.4.9 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)
- The merchant name may differ for other reasons (e.g. if the merchant uses multiple Acquirers, each of whom populate the merchant name slightly differently)
- The transaction amount may vary within reasonable expectations (see principle 14 in Table 27 in section 4.2.4.3)

### 4.6.5 Handling transactions from merchants who are not prepared for PSD2 or incorrectly submit transactions

There is a probability that not all merchants will be fully prepared for the application of PSD2 SCA by 14 September 2019. Issuers therefore need to set policies for handling transactions submitted without authentication and without correct exemption or out of scope indicators in

the authorization request. Blanket declines of such transactions may result in high levels of declines.

Visa's position is that Issuers should take advantage of any period of flexible enforcement allowed by NCAs in the particular country concerned to the greatest extent permitted to avoid high levels of declines due to merchant unpreparedness.<sup>63</sup> However, Visa encourages Issuers to apply risk solutions available to them to risk assess transactions before deciding whether to authorize or decline.

Issuers are also reminded that to assist merchant who are not ready to send a valid transaction identifier in MITs, Visa has assigned transaction identifiers 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 3.10.2 for more details.

## 4.7 3DS and authorization fall-back options

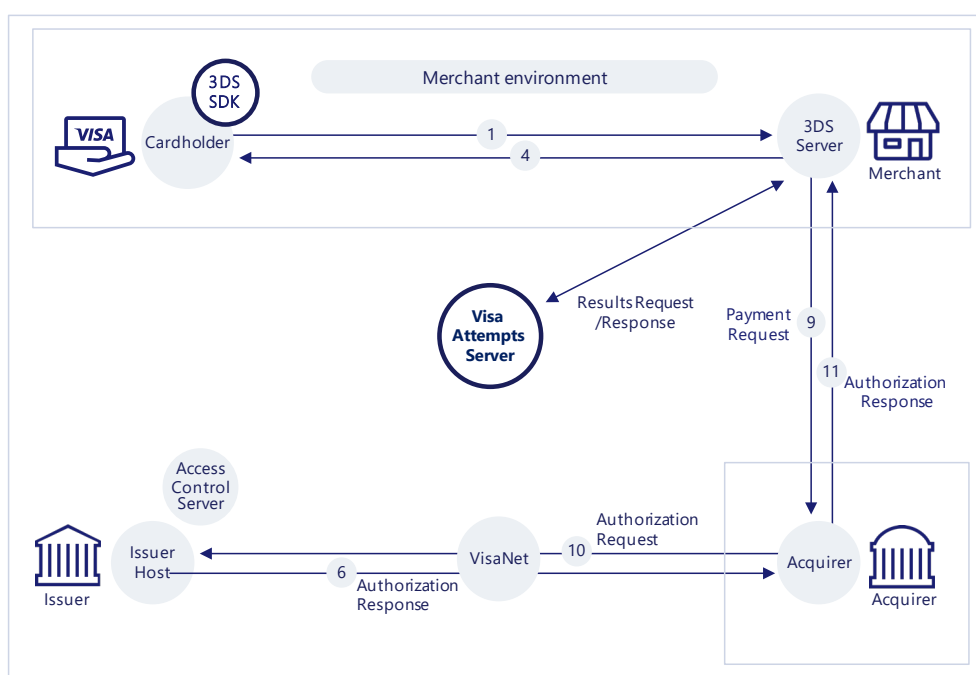


If for any reason an Issuer is unable to authenticate a transaction using 3DS, or is unable to respond to an authorization request, Visa will step in through application of the Visa Attempts Server or Stand-in Processing Service (STIP) respectively.

### 4.7.1 The Visa Attempts Server

The Visa attempts server will respond to an authentication request if the Issuer does not support EMV 3DS (applicable from April 2019), or the Issuer's ACS is unavailable or does not respond in time. 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.

**Figure 22: The role of the Visa Attempts Server**

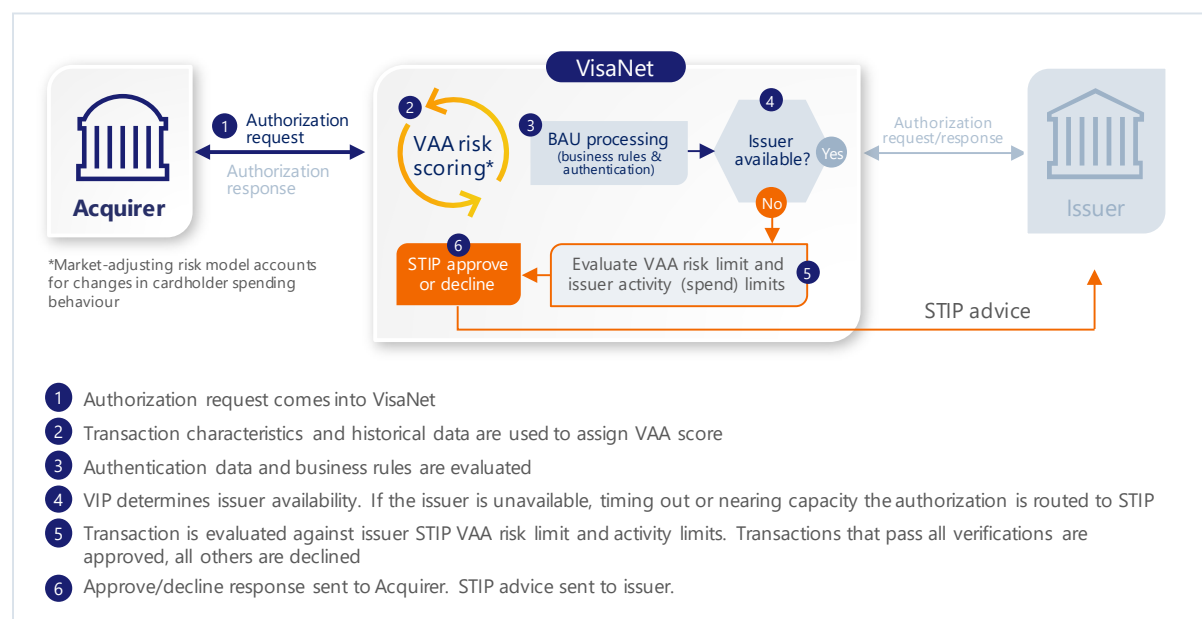


<sup>63</sup> See section 2 for more information on PSD2 SCA enforcement timescales

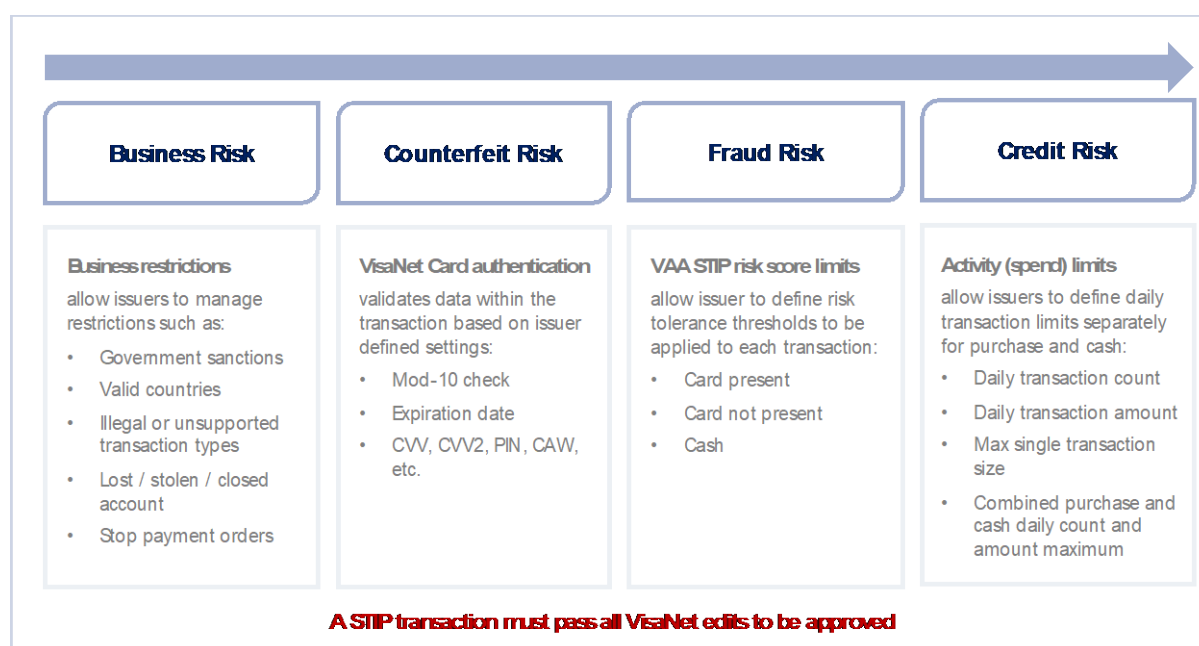
## 4.7.2 STIP

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 23: Operation of the STIP approval service**



**Figure 24: 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 25: An example set of STIP Limits for an Issuer's BIN**

<b>VAA Limits</b> <ul style="list-style-type: none"> <li>Card present, Card not present &amp; Cash</li> </ul> <b>Activity Limits</b> <ul style="list-style-type: none"> <li>Purchase &amp; Cash</li> <li>Count &amp; Amount</li> <li>Maximum single transaction amount</li> </ul> <b>Combined Maximums (Purchase &amp; Cash)</b> <ul style="list-style-type: none"> <li>Combined transaction count</li> <li>Combined transaction amount</li> </ul>	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 26: VisaNet STIP protects an Issuer's business**

<ul style="list-style-type: none"> <li>✓ It supports different limits for debit and credit portfolios for both purchase and cash transactions.</li> <li>✓ Issuers should review and update limits regularly in order to create a seamless customer experience.</li> <li>✓ 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.</li> <li>✓ It can perform cardholder validation and checks on behalf of issuers.</li> </ul>	<ul style="list-style-type: none"> <li>✓ 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.</li> <li>✓ 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.</li> </ul>
---	---

#### 4.7.2.1 Strong Customer Authentication Parameters for STIP<sup>64</sup>

To ensure that STIP transactions support the PSD2 requirement to enable Strong Customer Authentication (SCA), **effective with the April 2019 Business Enhancements release**, new SCA STIP parameters will be available for Issuers in the European Economic Area (EEA) in the following scenarios:

- Does the issuing Bank Identification Number (BIN) want to decline all Electronic Commerce Indicator (ECI) 6 e-commerce transactions without a valid exemption in STIP?

<sup>64</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

- Does the issuing BIN want to decline all ECI 07 e-commerce transactions without a Cardholder Authentication Verification Value (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 will be 'No'. For example, an ECI 06 e-commerce transaction without a valid exemption will not be declined in STIP due to SCA. 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. The questionnaire will be available to download from the Europe CIQ Forms page at Visa Online shortly.

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
- Response Code 1A: 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
- Delegated authentication

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.

#### 4.7.2.2 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 3.10.

## 4.8 Visa Direct and SCA under PSD2



### 4.8.1 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 33 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>

### 4.8.2 Visa Direct Transaction Types

Transactions associated with the Visa Direct service fall into two categories:

1. Original Credit Transactions (OCTs); used to “push” funds to a Visa cardholder’s account
2. Account Funding Transactions (AFTs); used to “pull” funds from a Visa cardholder’s account

These transaction types are defined below:

#### 4.8.2.1 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.

#### 4.8.2.2 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.

#### 4.8.2.3 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).

### 4.8.3 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.

#### 4.9 Visa Checkout and Visa Secure Remote Commerce



Merchants who use Visa Checkout to provide easy access to card payment and delivery data and a smoother checkout experience for their customers should be aware that using Visa Checkout alone does not fulfil their SCA obligations. Once the merchant has been provided with the payment credentials by Visa Checkout, authentication must still be sought (e.g. using 3DS) or a suitable exemption exercised.

Visa will soon be launching Visa Secure Remote Commerce, as part of a wider industry initiative in accordance with the specifications published by EMVCo. As Visa Checkout merchants are migrated to the Visa Secure Remote Commerce solution, the checkout services offered by Visa will continue to evolve.

#### 4.10 Visa Secure Authentication Technology and non-Visa Transactions



To maintain Visa Secure interoperability, effective 20 July 2019, 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>65</sup>.

---

<sup>65</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

---

The following subsections (starting at Section 5.2) provide merchants and Acquirers with best practice examples of how to ensure SCA is performed in compliance with PSD2 across common eCommerce payment scenarios, including MITs. The following information is provided for each payment scenario:

- A brief description introducing the payment scenario and when it is applicable, and
- When applicable, a step-by-step description of the actions that a merchant should take after each significant event (e.g. order is placed, shipment is made, etc.) occurs. The action taken by the merchant in each step is highlighted in bold and italics.

The approach for handling each of these scenarios serves only as a recommendation, therefore, merchants and Acquirers can choose alternative options that complement their business model, as long as they remain compliant with the key principles summarized in Section 4 and with any applicable laws, regulations and Visa Rules.

It is advisable that Issuers also familiarize themselves with the illustrated approach for handling each of the different eCommerce payment scenarios, so that they can adopt appropriate authorization policies to minimize unnecessary friction with their customers.

Before exploring individual payment scenarios, Section 5.1 explains the general approach across all scenarios for the inclusion of authentication-related data in the authorization message in order to achieve PSD2 SCA compliance and meet Visa acceptance requirements.

### 5.1 Inclusion of authentication-related data

A merchant and/or Acquirer must populate authorization messages with the correct authentication-related data to indicate to the Issuer one of the following:

- SCA has been performed, or
- An SCA exemption is being exercised, or
- SCA has not been performed or attempted and an exemption is not being exercised, for example, because the transaction is out of scope of SCA.

If a merchant, or Acquirer, fails to include the correct authentication-related data in the authorization for a transaction that is in scope, then the Issuer might decline the transaction, creating unnecessary friction for the cardholder.

The following subsections help merchants understand which authentication-related data must be populated in the authorization messages and whether they qualify for fraud liability protection, depending on:

- Whether the transaction is in scope of PSD2 and SCA,
- The type of payment credential being used (i.e. PAN or Token),
- The authentication method being used (i.e. via 3DS or VTS), and/or
- How any exemption is being exercised (via 3DS or directly in authorization)

Based on the above, the merchant can then use the tables described in the following subsections to determine which of the authentication-related data listed below is applicable, and therefore, must be populated in the authorization message:

- Exemption indicator in Field 34
- CAVV (in case of 3DS being used)
- TAVV (in case of token transactions)
- ECI value (can be either 05, 06 or 07)

### 5.1.1 Cardholder-Initiated Transaction (CITs)

Most CITs are in scope of SCA<sup>66</sup>. Therefore, depending on how SCA is being performed or exempted, the merchant must include the following in the authorization message for transactions of this type:

**Table 34 Authentication-related data required for CIT authorization messages**

Authentication scenario	Credential type	Exemption Indicator Required	CAVV required	TAVV required	ECI value	Fraud Liability Protection
SCA using 3DS	PAN or Token	No	Yes	For token only (can be CTF TAVV)	05 or 06	Yes
SCA exempted via 3DS	PAN or Token	Yes	Yes	For token only (can be CTF TAVV)	07	No
SCA exempted via authorization	PAN or Token	Yes	No	For token only (can be CTF TAVV)	07	No
SCA using VTS	Token	No	No	CTF TAVV	07	No

<sup>66</sup> CITs that are out of scope of PSD2, do not require SCA. Examples of CITs that are out of scope of PSD2 are One-Leg-Out transactions (although SCA should be applied on a "best efforts" basis)

## CAVV

- A CAVV can provide evidence of cardholder authentication or an applicable exemption to the Issuer.
- The merchant only receives fraud liability protection under the Visa Rules if the CAVV is provided with an ECI value of 05 or 06.
- If a CAVV was obtained, then the merchant should always include it in the authorization message, even if an exemption is being exercised or the transaction is out of scope of PSD2, to assist the Issuer in their authorization decision and prevent unnecessary declines.
- If an SCA exemption is exercised, then an applicable exemption indicator (in Field 34) along with an ECI of 07 and the CAVV, if available, must be included in the authorization message.

## TAVV

- All token transactions require the presence of a TAVV to support token domain controls, unless the transaction is a MIT, in which case a TAVV is not required (see Section 4.2.4.3 Principle 5).
- With exception of a TAVV generated under the Cloud Token Framework (see below), a TAVV cannot be used as evidence of SCA; therefore, a CAVV would still be required to provide evidence to the Issuer that SCA requirements are met.
- For token, an ECI is always supplied with the TAVV and should always be used unless overridden by the use of 3DS (for example, if VTS returns an ECI of 07 for a token transaction, but 3DS is also successfully used, the merchant can change the ECI 07 to an ECI 05 or 06, as directed by the 3DS transaction response).

## CTF TAVV

- In some cases, qualifying token requestors can use an enhanced version of the TAVV, known as the Cloud Token Framework (CTF) TAVV, as evidence of cardholder authentication (see Section 4.2.4.3 Principle 4). In such cases, a CAVV is not required for SCA compliance. This will always happen when a token requestor is participating in the Visa Delegated Authentication Program (VDAP)<sup>67</sup>

### 5.1.2 Merchant Initiated Transactions

MITs are out of scope of SCA<sup>68</sup>. Therefore, authentication data is not required in authorization messages for transactions of this type. As such, Issuers may not decline MITs with a response code 1A (SCA required), as the cardholder is not available for authentication during these transactions. The merchant must include the following in the authorization message for transactions of this type:

---

<sup>67</sup> For more information, please see the *Visa Delegated Authentication Implementation Guide*

<sup>68</sup> SCA must be performed for the CIT used to set up the MIT agreement in most cases. Applicable SCA exemptions can be exercised in some cases such as Reauthorization or Resubmission MITs. See Section 3.10 for all exceptions.



**Table 35 Authentication-related data required for MIT authorization messages**

Authentication scenario	Credential type	Exemption Indicator Required	CAVV required	TAVV required	ECI value	Fraud Liability Protection
MIT out of scope	PAN or Token	No	No	No	07	No

Note: Although MITs are out of scope of SCA, there is one special case where merchants can optionally include a CAVV in a Reauthorization MIT to qualify for fraud liability protection. More information on this is given in Section 5.1.3 below.

### 5.1.3 Reauthorization MIT (i.e. Delayed authorization with MRC 3903)

**A Reauthorization MIT can *optionally* include a CAVV for the sole purpose of qualifying the merchant for fraud liability protection.**

There are several payment scenarios in Section 5, where the merchant uses a Reauthorization MIT to complete the purchase, for example, when the shipment is split or is expected to be delayed. In such cases, the merchant does not authorize the transaction immediately because the authorization validity could expire before the shipment is ready, impacting the customer's open-to-buy for no valid reason. Instead, the merchant must complete the purchase transaction in two steps:

#### **Step A** - Perform a zero-value account verification

- An account verification is submitted at checkout following any required authentication and should contain the following:

**Table 36: Authentication-related data in account verification**

CAVV required	TAVV required	ECI value
No <sup>69</sup>	For token only (can be CTF TAVV)	07

- Issuers should not decline an account verification without a CAVV with a response code 1A (SCA required), since this is not a financial transaction.
- The account verification is the CIT used to set up the Reauthorization MIT (i.e. delayed authorization) in Step B.
- If the merchant requires fraud liability protection, it should not include the CAVV in the account verification, so that it can be included later in the delayed authorization (Step B).

<sup>69</sup> Merchants who wish to, can include the CAVV along with the obtained ECI value in the account verification. However, they must be aware of the implications of this approach, as described in Principle 13 of Section 4.2.4.3

### Step B – Submit delayed authorization with MRC 3903

- At a later stage, when the shipment is ready, the merchant submits a delayed authorization with Message Reason Code (MRC) 3903. The delayed authorization should contain the following depending on the authentication performed previously prior to the CIT:
- 

**Table 37: Authentication-related data in Reauthorization MIT**

Authentication scenario	Credential type	Exemption Indicator Required	CAVV required	TAVV required	ECI value	Fraud Liability Protection
SCA performed previously using 3DS	PAN or Token	No	Optional <sup>70</sup>	No	05 or 06, if CAVV present	Yes, if CAVV present
Any other scenario <sup>71</sup>	PAN or Token	Optional	No	No	07	No

- If the merchant has used 3DS to perform authentication, then the delayed authorization can optionally include a CAVV (with ECI 05 or 06) for the sole purpose of qualifying the merchant for fraud liability protection (see Principle 13 in Section 4.2.4.3 for more information).
- If an SCA exemption was exercised, then the applicable exemption indicator can be optionally included (in Field 34) in the authorization message, along with an ECI value of 07 and the CAVV, if available.

## 5.2 One-time purchase

A merchant receives an order from a customer for a known amount that it is able to fulfil in a single shipment within 7 days. For example a customer:

- checks out a basket of items online via a browser or mobile app
- purchases train tickets through an online booking service

<sup>70</sup> If the CAVV was submitted during the CIT, then the authorization can either be submitted with a new CAVV and associated ECI value (using 3RI, if available) or without a CAVV (in which case, without fraud liability protection).

<sup>71</sup> Other authentication scenarios refer to performing SCA via VTS or exempting SCA via 3DS or directly in authorization.

### Key Point

One-off transactions can be performed as a guest check out (POS entry mode = 01) or with a Credential-on-File (POS entry mode = 10). For more detail see Appendix A4: Stored Credential Framework

Scenario Steps
Customer places an Order
<ol style="list-style-type: none"> <li> <b>Authenticate customer</b> <ul style="list-style-type: none"> <li>The merchant <b>authenticates</b> the transaction immediately for the full amount, obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization.</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6</li> </ul> </li> <li> <b>Authorize transaction</b> <ul style="list-style-type: none"> <li>The merchant immediately <b>authorizes</b> the transaction for the full amount<sup>72</sup> and populates any applicable authentication-related data) in the authorization message as per Section 5.1.1</li> <li>If the transaction is out of scope of PSD2 SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.</li> </ul> </li> </ol>
Shipment made (Customer no longer available)
<ol style="list-style-type: none"> <li> <b>Clear funds</b> <ul style="list-style-type: none"> <li>The merchant ships the good(s) and <b>clears</b> the transaction for the full amount within 7 days.</li> </ul> </li> </ol>
Order Complete

## 5.3 Delayed Shipment

### 5.3.1 Delayed Shipment - expected delay

A merchant receives an order from a customer that it will fulfil in a single shipment, but it knows it will not be able to deliver within 7 days. The amount is known and not expected to change other than minimally due to, for example, shipping costs. Examples include:

- Item out of stock
- Pre-ordering upcoming goods or services such as new phone models or books / DVDs.

This approach is recommended so that the customer's open to buy is not impacted in the initial 7 days as the item will not be shipped within that period. If the authorization is to take place several months after initial order, it is best practice for the merchant to send a reminder

<sup>72</sup> Visa's view is that 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), however Merchants should check the position of individual National Competent Authorities. For more information see Section, 4.2.4.3 Principle 14.

to the cardholder a couple of days before authorization to maximize the opportunity for funds to be available.

**Note:** If the amount is not known at time of purchase, then the payment scenario described in Section 5.5 *Open orders - Unknown amount* applies.

Scenario Steps
Customer places an Order
<p><b>1. Authenticate customer</b></p> <ul style="list-style-type: none"> <li>The merchant <b>authenticates</b> the transaction immediately for the full amount, obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization.</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6</li> </ul>
<p><b>2. Perform a zero-value account verification</b></p> <ul style="list-style-type: none"> <li>The merchant must not authorize the transaction immediately as the authorization validity will expire before the shipment is ready and this would therefore impact the customer's open to buy for no valid reason.</li> <li>Instead, the merchant must perform a zero-value <b>account verification</b> to check that the card is valid and obtain an "initial" transaction ID and store it for use in step 3.</li> <li>The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3</li> </ul> <p>If a CAVV was obtained, the merchant should not include it in the account verification if it requires fraud liability protection. Instead they must store it for later use in the delayed authorization</p>
Merchant ready to make shipment (Customer no longer available)
<p><b>3. Submit delayed authorization with MRC 3903</b></p> <ul style="list-style-type: none"> <li>When the order is ready for shipment, the merchant <b>authorizes</b> for the full amount. The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework).</li> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3. If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.4.3 , Principle 12.</li> </ul>
Shipment made
<p><b>4. Clear funds</b></p> <ul style="list-style-type: none"> <li>The merchant <b>clears</b> the transaction for the full amount.</li> </ul>
Order Complete

### 5.3.2 Delayed Shipment - unexpected delay

Merchants should only perform authorization when they confirm that the goods are available and ready to be shipped (Section 4.2.4.3 Principle 10). However, if a merchant does authorize before confirming goods are available, Visa recommends it proceeds as follows. Merchants in this situation must be aware that 3DS v1.0 does not support 3RI or the ability to obtain a new CAVV required for fraud liability protection.

Scenario Steps
Customer places an Order
<p><b>1. Authenticate customer</b></p> <ul style="list-style-type: none"> <li>The merchant <b>authenticates</b> the transaction immediately for the full amount, obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization.</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6.</li> </ul>
<p><b>2. Authorize transaction</b></p> <ul style="list-style-type: none"> <li>The merchant immediately <b>authorizes</b> the transaction for the full amount<sup>73</sup> and populates any applicable authentication-related data in the authorization message as per Section 5.1.1:</li> <li>The merchant must also store the Transaction ID for this step in case it is required later.</li> <li>If the transaction is out of scope of PSD2 SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.</li> </ul>
End of 7 days Authorization validity period (Customer no longer available)
<p><b>3. Submit reversal</b></p> <ul style="list-style-type: none"> <li>After 7 days the merchant has been unable to ship the goods. The merchant must submit a <b>reversal</b> for the full transaction amount.</li> <li><b>Note:</b> The merchant could submit the reversal earlier as soon as they are aware that the shipment will be delayed beyond 7 days.</li> </ul>
Merchant ready to make shipment (Customer no longer available)
<p><b>4. Submit delayed authorization with MRC 3904</b></p> <ul style="list-style-type: none"> <li>When the order is ready for shipment, the merchant <b>authorizes</b> for the full amount<sup>73</sup></li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework)</li> <li>The merchant must populate any applicable authentication related data in the authorization message as per the Step B in Section 5.1.3</li> <li>In the unlikely event that the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.4.3, Principle 12.</li> </ul>
Shipment Made
<p><b>5. Clear funds</b></p> <ul style="list-style-type: none"> <li>The merchant <b>clears</b> the transaction for the full amount.</li> </ul>
Order Complete

<sup>73</sup> Visa's view is that 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), however Merchants should check the position of individual National Competent Authorities. For more information see Section, 4.2.4.3 Principle 14.

## 5.4 Split Shipment

### 5.4.1 Split Shipment - all fulfilled within 7 days

A merchant receives an online order from a customer for multiple items that it is able to fulfil within 7 days, but the goods are delivered in multiple shipments.

Scenario Steps
Customer places an Order
<b>1. Authenticate customer</b> <ul style="list-style-type: none"><li>The merchant <b>authenticates</b> the transaction immediately for the full amount, obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization.</li><li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6</li></ul>
<b>2. Authorize transaction</b> <ul style="list-style-type: none"><li>The merchant immediately <b>authorizes</b> the transaction for the full amount<sup>74</sup> and populates any applicable authentication-related data in the authorization message as per Section 5.1.1 If the transaction is out of scope of PSD2 SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.</li><li></li></ul>
Shipment Made (Customer no longer available)
<b>3. Clear funds for each shipment separately</b> <ul style="list-style-type: none"><li>The merchant <b>clears</b> for the amount of each shipment separately as and when they happen over the next 7 days using multiple clearing sequence numbers<sup>75</sup>.</li></ul>
Order Complete

Visa best practice is to use a single authorization with multiple clearing records for split shipment scenarios as defined in Section 4.2.4.3, Principle 10.

There is an alternative approach available for merchants who, due to their business processes, would prefer to submit multiple authorizations. For more information, refer to Section 5.4.3.

### 5.4.2 Split Shipment - partially fulfilled within 7 days (unexpected delay)

A merchant receives an order from a customer that it fulfils across multiple shipments, but some of those shipments unexpectedly take place more than 7 days after the initial order.

**Note:** Merchants who follow best practice and only perform authorization when they confirm that the goods are available and ready to be shipped (Section 4.2.4.3 Principle 10), will not find themselves in this position. Instead, they will either be able to confirm shipment straight away

<sup>74</sup> Visa's view is that 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), however Merchants should check the position of individual National Competent Authorities. For more information see Section, 4.2.4.3 Principle 14.

<sup>75</sup> For more information on how to handle multiple clearing records for a single transaction, refer to Visa Rules ID#0027756 and ID#0028914

(refer to Section 5.4.1) or they will identify a delay and therefore the need to perform multiple authorizations (refer to Section 5.4.3).

However, if a merchant does authorize before confirming goods available for shipping and then finds itself in this situation, Visa recommends it proceeds as follows. In this scenario, the merchant must be aware that 3DS v1.0 does not support 3RI or the ability to obtain a new CAVV required for fraud liability protection.

Scenario Steps
Customer places an Order
<b>1. Authenticate customer</b> <ul style="list-style-type: none"> <li>The merchant <b>authenticates</b> the transaction immediately for the full amount, obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization.</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6</li> </ul>
<b>2. Authorize transaction</b> <ul style="list-style-type: none"> <li>The merchant immediately <b>authorizes</b> the transaction for the full amount<sup>76</sup> and populates any applicable authentication-related data in the authorization message as per Section 5.1.1 <ul style="list-style-type: none"> <li>The merchant must also store the Transaction ID for this step in case it is required later.</li> <li>If the transaction is out of scope of PSD2 SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.</li> </ul> </li> </ul>
Merchant ready to make partial shipment (Customer no longer available)
<b>3. Clear funds for the amount of each shipment separately</b> <ul style="list-style-type: none"> <li>The merchant <b>clears</b> for the amount of each shipment separately using multiple clearing sequence numbers as and when each shipment occurs over the next 7 days<sup>77</sup>.</li> </ul>
End of 7 days Authorization validity period (Customer no longer available)
<b>4. Submit reversal</b> <ul style="list-style-type: none"> <li>At the end of 7 days, the order has only been partially fulfilled. The merchant submits a reversal for the amount of the original authorization that remains unfulfilled.</li> </ul> <p><b>Note:</b> The merchant could submit the reversal earlier as soon as they are aware that the shipment will be delayed.</p>
Merchant ready to make partial shipment (Customer no longer available)
<b>5. Submit delayed authorization with MRC 3903</b> <ul style="list-style-type: none"> <li>When each subsequent partial order is ready for shipment, the merchant authorizes for the amount relating to the goods included in the shipment.</li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework).</li> </ul>

<sup>76</sup> Visa's view is that 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), however Merchants should check the position of individual National Competent Authorities. For more information see Section, 4.2.4.3 Principle 14.

<sup>77</sup> For more information on how to handle multiple clearing records for a single transaction, refer to Visa Rules ID#0027756 and ID#0028914

- The merchant must populate any applicable authentication related data in the authorization message as per the Step B in Section 5.1.3

In the unlikely event that the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.4.3, Principle 12.

#### 6. Clear funds for the amount of each shipment separately

The merchant **clears** for the amount of each re-authorization as the related shipments are made.

Order Complete

### 5.4.3 Split Shipment - Multiple Authorizations

A merchant receives an order from a customer that they will fulfil across multiple shipments. Visa's best practice is to handle with one single authorization and multiple clearing as in scenario 5.3.1 and 5.3.2 above. If the order can be fulfilled in 7 days, the benefit of this approach is to avoid matching between a single authentication and multiple authorizations and minimize the need for the use of the MIT Framework. However, merchants whose business processes are such that they must request a new authorization for every shipment can do so as per the example below.

Scenario Steps	
Customer places an Order	
<b>1. Authenticate customer</b>	<ul style="list-style-type: none"> <li>• The merchant <b>authenticates</b> the transaction immediately for the full amount, obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization.</li> <li>• Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6</li> </ul>
<b>2. Either authorize transaction or perform a zero-value account verification</b>	<ul style="list-style-type: none"> <li>• Depending on whether the goods for inclusion in the first shipment are immediately available, the merchant must <i>choose one of the following options</i>: <ul style="list-style-type: none"> <li>a. Immediately <b>authorize</b> the transaction for the value of the goods to be shipped, if goods are available and store the "initial" transaction ID for later use in step 3 if further shipment(s) will be needed, or</li> <li>b. Perform a zero-value account verification, if none of the goods to be shipped are available.</li> </ul> </li> <li>• In case of <b>option (a)</b>: <ul style="list-style-type: none"> <li>○ The merchant must <b>authorize</b> immediately for the value of the goods to be shipped.</li> <li>○ The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1.</li> <li>○ If the transaction is out of scope of PSD2 SCA, then enough information must be included in the authorization to enable the identification of the transaction as out of scope.</li> </ul> </li> <li>• In case of <b>option (b)</b>: <ul style="list-style-type: none"> <li>○ The merchant must perform a zero-value <b>account verification</b> to check that the card is valid and obtain an "initial" transaction ID and store it for later use in step 3.</li> <li>○ The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.13.</li> <li>○ If a CAVV was obtained, the merchant should not include it in the account verification if they require fraud liability protection. Instead they must store it for later use in the delayed authorization.</li> </ul> </li> </ul>



Merchant ready to make shipments (Customer no longer available)	
<b>3. Submit delayed authorization with MRC 3903</b>	<ul style="list-style-type: none"> <li>When each of the remaining shipments is ready, the merchant <b>authorizes</b> <i>for the value of goods to be shipped</i>.</li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework). <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3</li> </ul> </li> <li>In the event that the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.4.3 Principle 12.</li> </ul>
<b>4. Clear funds</b>	<ul style="list-style-type: none"> <li>The merchant <b>clears</b> <i>the amount authorized as the related shipment is made</i>.</li> </ul>
Order Complete	

## 5.5 Open orders - Unknown final amount

The merchant receives an order with an initial amount that it expects to change significantly between receiving the initial order and the time of shipping.

For example, online groceries where the delivery date can be booked several days, weeks or even months in advance. The customer can come back and update the order as often as they like until the pre-agreed cut-off time. In addition, even after the order is complete, further variance may occur, due to item substitutions, inclusion of items priced by weight etc.

In this scenario, there are different options for the merchant to consider. The best option for a particular merchant will depend upon their preferred business processes.

In all cases, if the final authorization is to take place several weeks/months after initial order, it is best practice for the merchant to send a reminder to the cardholder a couple of days before authorization to maximize chances of funds being available.

## 5.5.1 Option 1: Delayed authorization, authenticate every order update

Scenario Steps	
Customer places an Order	
1. <b>Authenticate customer</b>	<ul style="list-style-type: none"> <li>The merchant <b>authenticates</b> the transaction immediately for the initial order amount, obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization.</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6.</li> </ul>
2. <b>Perform a zero-value account verification</b>	<ul style="list-style-type: none"> <li>The merchant must perform a zero-value <b>account verification</b> to check that the card is valid and obtain an "initial" Transaction ID and store it for later use. <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3.</li> <li>If a CAVV was obtained, the merchant should not include it in the account verification if they require fraud liability protection. Instead they must store it for later use in the delayed authorization.</li> </ul> </li> </ul>
Customer updates Order	
3. <b>Re-authenticate customer</b>	<ul style="list-style-type: none"> <li>Each time the customer comes back to adjust the order, the merchant performs another <b>authentication</b> for the new total cumulative amount, obtaining a new CAVV or CTF TAVV (and associated ECI value), discarding the initial one and keeping the latest one.</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6.</li> </ul>
4. <b>Perform an additional zero-value account verification (optional)</b>	<ul style="list-style-type: none"> <li>The merchant may also optionally perform an additional zero-value <b>account verification</b> each time to check that the card is valid. <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3.</li> <li>If a CAVV was obtained, the merchant should not include it in the account verification if they require fraud liability protection. Instead they must store it for later use in the delayed authorization.</li> </ul> </li> </ul>
Merchant ready to make shipment (Customer no longer available)	
5. <b>Submit delayed authorization with MRC 3903</b>	<ul style="list-style-type: none"> <li>At time of shipping, the order is closed. The merchant <b>authorizes</b> for the final amount<sup>78</sup>.</li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework) <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3</li> </ul> </li> <li>If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.4.3 Principle 12.</li> </ul>
6. <b>Clear funds</b>	<ul style="list-style-type: none"> <li>The merchant <b>clears</b> the transaction for the final amount.</li> </ul>
Order Complete	

<sup>78</sup> Visa's view is that 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), however Merchants should check the position of individual National Competent Authorities. For more information see Section 4.2.4.3 Principle 14.

## 5.5.2 Option 2: Authenticate for a maximum estimated amount upfront, delayed authorization

Scenario Steps
Customer places an Order
<p><b>1. Authenticate customer</b></p> <ul style="list-style-type: none"> <li>The merchant <b>authenticates</b> the transaction immediately for an estimated maximum amount that the basket can have obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization (see best practice below for additional considerations).</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6.</li> </ul>
<p><b>2. Perform a zero-value account verification</b></p> <ul style="list-style-type: none"> <li>The merchant must perform a zero-value <b>account verification</b> to check that the card is valid and obtain an “initial” Transaction ID and store it for later use. <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3.</li> <li>If a CAVV was obtained, the merchant should not include it in the account verification if they require fraud liability protection. Instead they must store it for later use in the delayed authorization</li> </ul> </li> </ul>
Customer increases order value
<p><b>3. Re-authenticate customer only if updated amount near or above original amount</b></p> <ul style="list-style-type: none"> <li>Each time the customer comes back to adjust the order, no further authentication is required unless the adjustment causes the order value to increase to near or above the originally authenticated amount.</li> <li>In which case, a new <b>authentication</b> must be performed for the new cumulative amount, obtaining a new CAVV or CTF TAVV (and associated ECI value), discarding the initial one and keeping this latest one.</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6.</li> </ul> <p><b>4. Perform an additional zero-value account verification (optional)</b></p> <ul style="list-style-type: none"> <li>The merchant may also optionally perform an additional zero-value <b>account verification</b> each time to check that the card is valid. <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3</li> <li>If a CAVV was obtained, the merchant should not include it in the account verification if they require fraud liability protection. Instead they must store it for later use in the delayed authorization</li> </ul> </li> </ul>
Merchant ready to make shipment (Customer no longer available)
<p><b>5. Submit delayed authorization with MRC 3903</b></p> <ul style="list-style-type: none"> <li>At time of shipping, the order is closed. The merchant <b>authorizes</b> for the final amount<sup>79</sup>.</li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework) <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3.</li> </ul> </li> </ul>

<sup>79</sup> Visa’s view is that 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), however Merchants should check the position of individual National Competent Authorities. For more information see Section 4.2.4.3, Principle 14.

- If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.4.3 Principle 12.

#### 6. Clear funds

- The merchant **clears** the transaction for the final amount.

Order Complete

### Best Practice

If using this option, clearly communicate to the customer before the authentication step that:

- they are authenticated for a maximum amount
- they will only be charged for what they purchase (which may be lower than the authenticated amount)
- no charges will appear on their card statement until the order is finalised

If you have clearly communicated a maximum to your customer at the previous authentication you should authenticate again as soon as that maximum is neared or exceeded. If the customer's reasonable expectations are that the amount authentication could be exceeded, then you can authorize a higher amount within the customer's reasonable expectations (with an upper limit of a 15% variance between authenticated and authorized amount) (see Section 4.2.4.3 Principle 14)

### 5.5.3 Option 3: Authenticate and use Incremental MIT to authorize amount above initial amount

This option is only applicable to specific Merchant Category Codes permitted to use Incremental MITs, as indicated in Visa Rule ID # 0025596, for example, online groceries.

Scenario Steps
Customer places an Order
<p><b>1. Authenticate customer</b></p> <p>The merchant <b>authenticates</b> the transaction immediately for an estimated maximum amount that the basket can have, obtaining a CAVV or CTF TAVV (and associated ECI value) for later submission in the authorization. The merchant must inform the customer that:</p> <ul style="list-style-type: none"> <li>○ this is an estimated amount,</li> <li>○ they will only be charged for what they purchase when the order is finalized and must inform the customer and get their consent that</li> <li>○ the final amount may be higher than estimated, either because cardholder may make addition to the basket and/or due to allowable variations within reasonable expectations (e.g. brand substitution, item not available etc.)</li> </ul> <ul style="list-style-type: none"> <li>• It is not permissible to use an exemption in order to skip authentication under this option, as authentication is necessary in order for the merchant to have the option of initiating an Incremental MIT at the time of shipping (see below).</li> </ul>
<p><b>2. Perform a zero-value account verification</b></p> <ul style="list-style-type: none"> <li>• The merchant must perform a zero-value <b>account verification</b> to check that the card is valid and obtain an "initial" Transaction ID and store it for later use. <ul style="list-style-type: none"> <li>○ The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3.</li> <li>○ If a CAVV was obtained, the merchant should not include it in the account verification if they require fraud liability protection. Instead they must store it for later use in the delayed authorization.</li> <li>○ The Transaction ID for this authorization is stored for later use.</li> </ul> </li> </ul>
Customer increases order value to greater than the authenticated amount
<ul style="list-style-type: none"> <li>• Each time the customer comes back to adjust the order, no further authentication is required.</li> <li>• The merchant may optionally perform an additional zero-value <b>account verification</b> each time to check that the card is still valid. <ul style="list-style-type: none"> <li>○ The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3.</li> </ul> </li> </ul>
Merchant ready to make shipment (Customer no longer available) – amount lower or up to a maximum 15% higher than the authenticated amount <sup>80</sup>
<p><b>3. Submit delayed authorization with MRC 3903</b></p>

<sup>80</sup> Visa's view is that 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), however merchants should check the position of individual National Competent Authorities. For more information see Section 4.2.4.3, Principle 14

<ul style="list-style-type: none"> <li>At time of shipping, the order is closed. The merchant <b>authorizes</b> <i>for the final amount</i><sup>81</sup>.</li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework) <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3.</li> </ul> </li> <li>If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.4.3 Principle 12.</li> </ul>
<p><b>4. Clear funds</b></p> <p>The merchant <b>clears</b> <i>the transaction for the final amount</i>.</p>
<p><b>Merchant ready to make shipment (Customer no longer available)- amount greater than the authenticated amount</b></p>
<p><b>3. Submit two authorizations</b></p> <ul style="list-style-type: none"> <li>At time of shipping, the order is closed. The merchant <b>authorizes</b> <i>for the estimated amount authenticated</i>.</li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 2 (as per MIT Framework) <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3.</li> <li>If the shipment is delayed by 90 days or more, the merchant must perform additional action to ensure that the transaction is able to continue, as defined in Section 4.2.4.3 Principle 12.</li> </ul> </li> <li>The merchant must also submit a second authorization for the additional amount not authenticated, but using the message reason code 3900- MIT Incremental. <ul style="list-style-type: none"> <li>Merchant should discuss with their Acquirers to be familiar with the rules associated with the use of Incremental transactions for their MCC.</li> <li>The merchant must populate any applicable authentication-related data in the authorization message as per section 5.1.2.</li> </ul> </li> </ul>
<p><b>4. Clear funds</b></p> <p>The merchant <b>clears</b> <i>the transaction for the final amount</i>.</p>
<p><b>Order Complete</b></p>

## 5.6 Aggregated payments

Visa rules define an aggregated payment as a single transaction that combines multiple purchases made by the same cardholder on the same payment credential (which may be updated from time to time) at the same merchant during a defined time period and up to a defined amount (refer to Visa rule ID # 0024270).

Visa allows aggregation of payments for ecommerce merchants, typically capped at 15USD (or local currency equivalent) or 7 days whichever comes first. However, these terms vary for some MCCs and some disclosure requirements and receipt requirements apply (refer to Visa Rule ID # 0002906 and # 0028052).

In this scenario, a merchant handles micro-payments and only charges the customer when reaching a pre-agreed total or at a specific time. The charge occurs when the cardholder is not

<sup>81</sup> Visa's view is that 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), however merchants should check the position of individual National Competent Authorities. For more information see Section 4.2.4.3, Principle 14

available. The exact time and amount can vary based on market and MCC, but for the purposes of these examples a time limit of 7 days is used.

When considering how best to handle aggregated payments for their business model, the merchant can choose from the following options.

#### 5.6.1 Option 1: Merchant sets up customer agreement to enable payments under MIT Unscheduled Subscription type (UCOF)<sup>82</sup>

A merchant storing a Credential-on-File for aggregated payments could process orders as Unscheduled Credential-on-File (UCOF) MITs by setting up an agreement with the cardholder. This approach is suitable for use cases such as bike or car sharing, where the customer is not directly engaging with the merchant in a manner which allows authentication to take place. For further details see Section 3.10.

---

<sup>82</sup> Visa reserves the right to revise this guide pending further regulatory developments.

## 5.6.2 Option 2: Authentication for fraud liability protection

Scenario Steps	
Customer makes purchase that triggers a new aggregation series	
1. <b>Notify customer of payment levy conditions</b>	<ul style="list-style-type: none"> <li>Merchant <b>informs</b> cardholder that payment will be levied either when transactions cumulate to 15 USD (or local currency equivalent) or at 7 days, whichever comes first.</li> </ul>
2. <b>Authenticate customer</b>	<ul style="list-style-type: none"> <li>Merchant <b>authenticates</b> for 15 USD (or local currency equivalent) obtaining a CAVV or CTF TAVV (and associated ECI value).</li> <li>Applicable exemptions can be exercised which may result in this step being skipped, see Section 4.2.6.</li> </ul>
3. <b>Perform a zero-value account verification</b>	<ul style="list-style-type: none"> <li>The merchant must perform a zero-value <b>account verification</b> to check that the card is valid and obtain an "initial" Transaction ID and store it for later use. <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3.</li> <li>If a CAVV was obtained, the merchant should not include it in the account verification if they require fraud liability protection. Instead they must store it for later use in the delayed authorization.</li> </ul> </li> </ul>
Aggregated value or time threshold reached (Customer no longer available)	
4. <b>Submit delayed authorization with MRC 3903</b>	<ul style="list-style-type: none"> <li>When either threshold is reached, the merchant <b>authorizes</b> for the final amount.</li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from step 3 (as per MIT Framework) <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3</li> </ul> </li> <li>If the authorization is declined, as the goods and services have already been provided to the customer, the merchant may <b>resubmit</b> the transaction indicated with MRC 3903 to recuperate the funds, providing that the original decline response code indicates that the Issuer may approve a future transaction.</li> </ul>
5. <b>Clear funds</b>	<ul style="list-style-type: none"> <li>The merchant <b>clears</b> the transaction for the full cumulative amount.</li> </ul>
Customer makes purchase that triggers a new aggregation series	
6. <b>Restart from step 1</b>	



### 5.6.3 Option 3: Authorize for the maximum amount upfront, authenticate only if required by the Issuer

Whilst it is possible for an Issuer to immediately authorize for the full amount upfront, requesting a suitable SCA exemption and then only authenticating if required by the Issuer, and clearing the transaction when the 15USD total is reached or at 7 calendar days, this is not Visa's recommended approach, since it:

- Immediately impacts the customer's open to buy, in particular if the customer has limited cash flow
- Does not provide a convenient user experience when authentication is required
- Increases the chance that an Issuer will decline the transaction

Therefore, this approach should only be used if the merchant has no other option.

### 5.7 Real-time service via mobile app with payment after service /completion

In these scenarios, the customer is paying for a service at end of service rendered. Examples include:

- Ordering a car ride via a mobile app
- Opening a fuel pump and buying fuel via a mobile app

In such cases, the amount can be estimated at the start, but the final amount is not known at time of order. Payment is not made on booking, but at service completion.

**Note:** The rest of this section assumes that Unscheduled Credential-on-File (UCOF) MITs are not suitable for this type of scenario, since it involves a merchant/cardholder interaction via a mobile app where authentication is possible.

The example scenarios assume that any variation between the original and final amount is within the customer's reasonable expectations<sup>83</sup>. In the case where the final value of the transaction is outside of the customer's reasonable expectations then additional authentication and authorization may be needed. For more information on reasonable expectations see Section 4.2.4.3 Principle 14.

---

<sup>83</sup> Visa's view is that it is permissible for the amount in authentication and authorization to vary within the customer's reasonable expectations, however merchants should check the position of individual National Competent Authorities.

### 5.7.1 Option 1: Direct to authorization flow

In this Scenario, if an SCA exemption can be exercised then the merchant can request it via the direct to authorization flow, in order to enable authentication to be by-passed, unless ultimately required by the Issuer.

Scenario Steps	
Customer books service	
1. <b>Authorize transaction</b>	<ul style="list-style-type: none"> <li>Merchant <b>authorizes</b> for <i>highest estimated amount of the service at booking</i>, claiming appropriate exemption and using the estimated amount indicator (refer to Base I Technical Specification Volume 1 for further details). <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1. Refer to the authentication scenario "SCA exempted via authorization" in Table 34</li> </ul> </li> <li><b>Note:</b> Using an estimated amount is only available to certain merchant types, such as taxis, hotels etc. See Visa Rule # 25596.</li> </ul>
2. <b>Authenticate customer if Issuer responds with 1A</b>	<ul style="list-style-type: none"> <li>If the transaction is approved, skip to step 3 or 4 as applicable.</li> <li>However, if the Issuer responds with a response code 1A – SCA required then the merchant performs <b>authentication</b> for the <i>estimated amount</i>, obtaining the CAVV or CTF TAVV and associated ECI value, and then <b>authorizes</b> again. The estimated indicator must again be populated in the authorization.</li> </ul>
Final value of service not within reasonable expectations	
3. <b>Submit reversal and authorize final amount</b>	<ul style="list-style-type: none"> <li>If the final amount is above the customer's reasonable expectations (as described in Principle 14<sup>84</sup>) compared to the authorized amount, then the merchant must: <ul style="list-style-type: none"> <li><b>Reverse</b> the authorization from step 1 or 2</li> <li><b>Authorize</b> for the <i>final amount</i> using applicable exemption flags in Field 34. <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1. Refer to the authentication scenario "SCA exempted via authorization" in Table 34.</li> <li>If no exemptions can be exercised or the Issuer responds with a response code 1A (SCA required), then the merchant must contact the cardholder (either sending a message or waiting for next usage of the app as most appropriate with business model) to authenticate prior to attempting another authorization. (If a CAVV was obtained in step 2 it is no longer valid as not covering the final amount and should not be used in this authorization).</li> </ul> </li> </ul> </li> </ul>
4. <b>Clear funds</b>	<ul style="list-style-type: none"> <li>The merchant <b>clears</b> the <i>transaction for the final amount</i> (within reasonable customer expectations as described in Principle 14, Section 4.2.4.3). The final amount could include a tip, for example.</li> </ul>
Final value of service within reasonable expectations	
3. <b>Clear funds</b>	<ul style="list-style-type: none"> <li>The merchant <b>clears</b> the <i>transaction for the final amount</i> (within reasonable customer expectations as described in Principle 14<sup>84</sup>, Section 4.2.4.3). The final amount could include a tip, for example.</li> </ul>
Order Complete	

<sup>84</sup> Visa's view is that 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), however Merchants should check the position of individual National Competent Authorities.

## 5.7.2 Option 2: Perform authentication every time

Scenario Steps	
Customer books service	
1. <b>Authenticate customer</b>	<ul style="list-style-type: none"> <li>Merchant <b>authenticates</b> for highest estimated amount at ordering, obtaining a CAVV or CTF TAVV (and associated ECI value). In such cases, the merchant should communicate to the cardholder prior to authentication that they are being authenticated for a maximum amount (which must be specified) and that no charges will appear on their card statement until the order is finalized.</li> </ul>
2. <b>Either authorize transaction or perform a zero-value account verification</b>	<ul style="list-style-type: none"> <li>Merchant can choose one of the following options: <ul style="list-style-type: none"> <li>a. <b>Authorize immediately</b> for highest estimated amount at ordering.</li> <li>b. Perform a zero-value <b>account verification</b> and later <b>submit a delayed authorization with MRC 3903</b></li> </ul> </li> <li>In case of <b>option (a)</b>: <ul style="list-style-type: none"> <li>The merchant must <b>authorize</b> immediately for highest estimated amount at ordering.</li> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1.</li> <li>Merchant must use the estimated amount indicator (refer to Base I Technical Specification Volume 1 for further details).</li> <li><b>Note:</b> Using an estimated amount is only available to certain merchant types, such as taxis, hotels etc. See Visa Rule # 25596</li> </ul> </li> <li>In case of <b>option (b)</b>: <ul style="list-style-type: none"> <li>The merchant must perform a zero-value <b>account verification</b> to check that the card is valid and obtain an "initial" transaction ID and store it for use in the later authorization.</li> <li>The merchant must populate any applicable authentication-related data in the account verification as per Step A in Section 5.1.3.</li> <li>If a CAVV was obtained, the merchant should not include it in the account verification if they require fraud liability protection. Instead they must store it for later use in the delayed authorization.</li> </ul> </li> </ul>
Final value of service not within reasonable expectations	
3. <b>Authorize final amount using exemption or new authentication</b>	<ul style="list-style-type: none"> <li>If the final amount is above the customer's reasonable expectations (as described in Principle 14<sup>85</sup>, Section 4.2.4.3) compared to the authorized amount, then: <ul style="list-style-type: none"> <li>If <b>option (a)</b> was chosen in step 2, then the merchant must first <b>reverse</b> the authorization</li> <li>The merchant <b>authorizes</b> for the final amount. The CAVV from step 1 is no longer valid as not covering the final amount and should not be used in this authorization. Any applicable exemptions should be exercised to minimize the chance of the Issuer declining due to a lack of authentication. If it is a token transaction, a TAVV must be included.</li> <li>If the Issuer responds with a response code 1A (SCA required), then the merchant must contact the cardholder (either sending a message or waiting for next usage of the app as most appropriate with business model) to <b>authenticate</b> prior to attempting another authorization for the final amount.</li> </ul> </li> </ul>
4. <b>Clear funds</b>	<ul style="list-style-type: none"> <li>The merchant <b>clears</b> the transaction for the final amount.</li> </ul>

<sup>85</sup> Visa's view is that 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), however Merchants should check the position of individual National Competent Authorities.

Final value of service within reasonable expectations	
3. <b>Submit delayed authorization with MRC 3903</b>	<ul style="list-style-type: none"> <li>If <b>option (a)</b> was chosen in step 2, then proceed to step 6.</li> <li>If <b>option (b)</b> was chosen in step 2, then the merchant <b>authorizes</b> for the final amount.</li> <li>The authorization must include a message reason code of 3903 to indicate that the customer is no longer present and the Transaction ID from the account verification (as per MIT Framework) <ul style="list-style-type: none"> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Step B in Section 5.1.3</li> </ul> </li> </ul>
4. <b>Clear funds</b>	<ul style="list-style-type: none"> <li>The merchant <b>clears</b> the transaction for the final amount (within reasonable customer expectation).</li> </ul>
Order Complete	

### 5.7.3 Option 3: Authenticate and use Incremental MIT to authorize amount above initial amount

This option is only applicable to specific Merchant Category Codes (MCC, e.g. card absent transactions at a taxi operator) permitted to use Incremental MITs, as indicated in Visa Rule ID # 0025596.

Scenario Steps
Customer books service
<p>This step is only required when new credentials are captured for the first time (new stored credential agreement),</p> <p><b>1. Cardholder accepts T&amp;Cs for MIT Incremental agreement</b></p> <ul style="list-style-type: none"> <li>Merchant discloses to cardholder appropriate T&amp;Cs. any other requirements associated with the storage of the credentials.</li> <li>The customer must explicitly accept the T&amp;Cs for the agreement to proceed.</li> </ul> <p>This step is only required when new payment credentials are captured.</p>
<p><b>2. Authenticate customer</b></p> <ul style="list-style-type: none"> <li>Merchant <b>authenticates</b> for initial or estimated amount at ordering, obtaining a CAVV or CTF TAVV (and associated ECI value) – exemptions cannot be used if the merchant wishes the ability to process any incremental transaction later.</li> </ul>
<p><b>3. Authorize transaction with estimated indicator</b></p> <ul style="list-style-type: none"> <li>The merchant immediately <b>authorizes</b> the transaction for the initial or estimated amount at ordering, <b>using the estimated indicator</b> (no incremental transaction can be processed later unless preceded by an estimated authorization). <ul style="list-style-type: none"> <li>The merchant must inform the customer that if the final amount is higher than estimated, customers agrees to pay for final amount as long as within reasonable cardholder expectation. <ul style="list-style-type: none"> <li>Merchant should discuss with their Acquirers to be familiar with the rules associated with the use of Incremental transactions for their MCC.</li> </ul> </li> <li>The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1. Exemptions cannot be used if the merchant wishes to have the ability to process any incremental transaction.</li> </ul> </li> </ul>

- If this is the first transaction, the appropriate indicator must also be populated to indicate that credentials are being stored. For more information about the Stored Credential Framework and the requirements a merchant must meet, see Appendix A.4
- The Transaction ID for this authorization is stored for later use.

Final value of service is higher than 15%<sup>86</sup> of amount of initial authorization from step 3

**4. Perform an incremental authorization using the MIT Framework**

- If the final amount on service completion is higher than the amount initially authenticated by more than 15% (or appropriate percentage for this MCC according to Visa Rules ID # 0025596), the merchant must perform an **incremental authorization using the MIT Framework** for the additional amount not yet authorized in step 3.
- The authorization must include a message reason code of 3900 to indicate that the customer is no longer present and the Transaction ID from step 3 (as per MIT Framework).
  - The merchant must populate any applicable data in the authorization message as per Section 5.1.2.

**5. Clear funds**

The merchant **clears** the transaction for the final amount.

Final value of service within 15%<sup>86</sup> of initial authorization from step 3

**4. Clear funds**

- The merchant **clears** the transaction for the final amount.

Note that if the initial authorization from step 3 was for a higher amount than the amount cleared, the merchant must also submit a reversal for the difference. Please refer to Visa rule ID #0025597 for more information.

Order Complete

<sup>86</sup> Please note this percentage varies depending on the MCC, please refer to Visa Rules (ID # 0025596) for appropriate percentage.

## 5.8 Omni-channel purchases

There are certain scenarios where a merchant chooses to deliver goods or services via a mixture of remote and face-to-face experiences. Such omni-channel use cases are becoming more and more common, and also need to be SCA compliant.

### Key Point

The authentication for a delivery does not have to be performed online but can be delayed until later face-to-face interaction. Equally an authentication performed on-line can be leveraged to enhance later face-to-face delivery or in store pick-up of goods and services.

#### 5.8.1 Reserve on-line, pay in store

A customer places an order via a website or mobile app but not perform any authentication or authorization online. In this case, all authentication and authorization would be performed in store, as part of a face-to-face transaction. For example, a customer could reserve stock for collection within 24 hours at a general-purpose store, performing a Chip and PIN transaction at time of collection to meet SCA requirements.

#### 5.8.2 Buy online, pick up in store (BOPIS)

A customer places an order via a website and complete authentication and authorization online (as per the one-time purchase scenario defined in Section 5.2).

The merchant would then need to have in place a mechanism to tie up the order with the customer at time of collection, for example:

- Purchase clothes online for collection in store, with customer presenting an order reference number or proof of ID to enable collection
- Buying cinema tickets online for collection from automated machines that use the card used to pay online to identify the customer and deliver the tickets

In this case, it is the online experience that manages authentication and authorization, therefore the transaction is treated as eCommerce, not face-to-face.

#### 5.8.3 Pay in-app when in store

A customer uses a mobile app check-out experience to pay for goods in store. From a transaction authentication point of view, this should be considered the same as BOPIS. The in-app transaction is the environment where authentication and authorization are performed, and therefore the transaction is treated as eCommerce, not face-to-face.

#### 5.8.4 Pay in store for home delivery

A customer purchases goods in store for home delivery, completing the authentication and authorization face-to-face, but with the order being fulfilled through the merchant's eCommerce home delivery processes. For example, a customer wishing to buy a pair of shoes goes into a store, but their size is out of stock. The merchant guides them through a process using a tablet-based POS to purchase the desired size for home delivery. Payment is completed with the merchant face-to-face as a Chip and PIN transaction, meeting SCA requirements.

#### 5.9 Resubmission of declined authorization on contactless transit transactions

Resubmissions are a type of transaction whereby the merchant can re-submit a previously declined authorization due to lack of funds in the case **of contactless transactions performed in the transit environment where a service has already been delivered**. For example, if a cardholder taps into a mass transit gate with their Visa card or token on a mobile device, but at the end of day authorization is declined by the Issuer due to lack of funds. In these circumstances, the Mass Transit merchant is allowed to resubmit the authorization after an agreed period of time to attempt to collect the funds owed. In this case, the original CIT is exempt from SCA under the unattended terminals for transport fares and parking fees exemption and the Resubmission (which can only be performed as card not present since the contactless authentication data has already been used once) is simply an attempt to complete that already exempted transaction. Therefore, no SCA data needs to be included in the resubmission.

The merchant must identify the Resubmissions follows using the Transaction ID from the declined contactless authorization as the original Transaction ID.

**Table 38: Resubmission**

Description	Transaction Type	POS Entry Mode (PEM) (F22)	POS Environment (F126.13)	Message Reason Code (F126.13)	Transaction ID (F125**)
Resubmission	First Transaction (CIT)	07	--	--	--
	Subsequent Transactions (MIT)	01	--	3901	Tran ID of First transaction

### Key Point

Resubmissions **must not** be used for declined authorizations *where the services (or goods) have not yet been delivered*. For example, a customer attempts to purchase goods online at a merchant; however, the authorization is declined due to lack of funds. At this point, the goods have not yet been shipped. In this case, for the transaction to complete, the customer must either provide a different payment credential or replenish funds prior to the merchant submitting a new authorization request.

In the case of an MIT other than Resubmission being declined, a Resubmission must never be used. For example, if a merchant charges in advance for a service subscription using a recurring MIT. If the recurring transaction MIT is declined, depending on the decline response code, the merchant may later attempt a new authorization request as a recurring MIT for that subscription charge, until it is either approved or a maximum retry limit is reached. Refer to Visa rule # 6007 for more information.

#### 5.10 Accessing stored credentials using QR codes

Some merchants provide proprietary closed-loop payment solutions through their mobile app by enabling the customer to initiate a transaction using a QR code<sup>87</sup>. Examples include apps that generate a QR code which can be presented to the merchant in-store, or apps that read a QR code printed on a utility bill or similar payment request. The QR code subsequently enables the merchant back-end systems to identify a stored credential. Such an approach enables the merchant to enrich the customer experience by providing mobile app features such as loyalty.

Merchants using this kind of solution must be aware that as CITs using stored credentials, such transactions still require SCA, or an applicable exemption. The precise means by which a merchant achieves this will be implementation specific, but Visa provides a number of tools that could help:

- **3D Secure:** Integration with 3DS can meet SCA requirements and EMV 3DS 2.1.0 and above is optimized for mobile-based solutions.
- **Delegated Authentication:** Both 3DS and the Visa Token Service can be used to enable participation in the Delegated Authentication Program, giving merchants the opportunity to control the SCA experience for their customers. For more information on Visa Delegated Authentication, please Section 3.8.
- **Use of the Trusted Beneficiaries Exemption:** Encouraging customers to register the merchant as a trusted beneficiary with their Issuer, where the Issuer supports the exemption, to maximize the possibility of being able to exercise the trusted beneficiary exemption<sup>88</sup>

---

<sup>87</sup> There is an EMVCo Specification for supporting open-loop in-store payments using QR codes, but it is only supported in a limited number of global markets, none of which are in the European region.

<sup>88</sup> Note that Issuers are not obliged to provide a trusted beneficiary capability and those that do may still choose not to apply it for every transaction where it is requested



## 5.11 Establishing a new agreement for future MITs

Upon establishing an agreement to process future MITs, a merchant must authenticate and authorize for the amount being collected at the time of the agreement and disclose appropriate T&Cs related to the agreement as described below. In a few select cases, SCA may not be required if an exemption can be applied. Please refer to Section 3.10 for information on those specific cases.

### 5.11.1 SCA is required by merchant to set up new agreement

Scenario Steps	
Customer Signs up to a new agreement for future merchant-initiated payments	
1. <b>Cardholder accepts T&amp;Cs for MIT agreement</b>	<ul style="list-style-type: none"><li>The merchant discloses to the cardholder appropriate T&amp;Cs and follows other requirements associated with the future MIT type it will process.</li><li>The customer must explicitly accept the T&amp;Cs for the agreement to proceed.<ul style="list-style-type: none"><li>Merchants should discuss with their Acquirers and be familiar with the rules associated with their MIT types. For more information, see Appendix A.4, Appendix A.6 and Section 5.13.</li></ul></li></ul>
2. <b>Authenticate customer</b>	<ul style="list-style-type: none"><li>When setting up an agreement to process future MITs, the merchant <b>authenticates</b> <i>for the amount due immediately only (if no amount is due, authentication must be performed with "zero" as the amount)</i> as per Section 4.2.4.3, Principle 17, applying SCA.</li><li><b>Note:</b> SCA exemptions cannot be exercised when setting up a new MIT agreement except:<ul style="list-style-type: none"><li>For Reauthorization and Resubmission MITs, where applicable exemptions can be exercised in the original CIT used to set up future MITs of these types.</li><li>During a booking made via a secure corporate payment process that qualifies for application of the secure corporate payments processes and protocols exemption. Refer to Section 3.10 for details on the use cases where exemptions can be used.</li></ul></li></ul>
3. <b>Authorize transaction</b>	<ul style="list-style-type: none"><li>The merchant <b>authorizes</b> <i>for the amount due immediately (which, as noted above, must be zero if no amount is due)</i> and populates any applicable authentication-related data in the authorization message as per Section 5.1.1, taking into account the fact that SCA exemptions cannot be exercised when setting up a new agreement (except in the cases stated in Section 3.10).<ul style="list-style-type: none"><li>The merchant must store the Transaction ID of this authorization for later use as the Initial Tran ID in future MITs<sup>89</sup>.</li><li>If zero, or a discounted, amount is due immediately (e.g. as part of an introductory/promotional offer), then authorize only for the amount due immediately (i.e. for zero or discounted amount) as per Section 4.2.4.3, Principle 17.</li><li>This first authorization is the CIT used to establish the agreement for future MITs and should be flagged as per the key data fields detailed in Section 3.10.2 Table 22</li><li>If the authorization is approved, the payment credentials can be stored for future use according to the Stored Credential Framework if appropriate (see Appendix A.4:)<sup>90</sup>.</li><li>If the credential is not stored under the Stored Credential Framework, the details can be kept but only as long as required in order to complete the current transaction agreement (e.g. to process any Industry Specific MITs such as No Shows, Incremental Authorizations or Resubmissions).</li></ul></li></ul>

<sup>89</sup> If the agreement was established prior to 14 September 2019, then Grandfathering applies. See Section 4.2.4.3, Principle 16

<sup>90</sup> The credential must be stored according to the Stored Credential Framework for Standing Instruction MITs. For industry best practice, use of stored credential is optional.

### Customer uses service leading to additional payments

#### 4. Authorize using MIT Framework

- Depending on the MIT type, the merchant must communicate with the cardholder, if required, prior to processing an MIT (see Section 5.13 for examples).
- Merchant **authorizes** MITs, identified as shown in Section 3.10.2 Table 22. The initial Tran ID to use is the one generated in step 3 or the Tran ID of a previous MIT can be populated instead, or for an interim period if the merchant does not have any previous Tran ID available, a Visa Acquirer-assigned interim Tran ID can be used if supported by the Acquirer.
- *The amount in future MITs may vary from the original amount as long as the amount calculation method is disclosed to the customer in the T&Cs of the established agreement and the amount authorized is within reasonable customer expectation.*
- It is important for merchants to be aware, however, that MITs do not have fraud liability protection under the Visa Rules. No CAVV or TAVV is required to be included in the authorization, as the MIT is out of scope of PSD2 SCA. Refer to Section 5.1.2 for more information.

#### 5. Clear funds

- Merchant **clears** the transaction for the final amount in the MIT.

### 5.11.2 Agreements established by mail order or telephone order (MOTO)

Sometimes a cardholder establishes an agreement with a merchant over the phone, by mail or email. In those cases, setting up the agreement is recorded as a MOTO type transaction. When this is the case, it is important for merchants to remember that the subsequent payments made under that agreement are not to be flagged as MOTO. They are MITs:

- When an agreement is initiated via MOTO, this initial CIT is to be indicated as MOTO and is out of scope of SCA.
- The ongoing transactions must be flagged with the appropriate MIT type (see Section 3.10) and not as a MOTO transaction. MITs are considered by Visa out of scope of PSD2, so SCA is not required.

#### Key Point

When setting up an MIT agreement, MOTO is only valid for the initial transaction when an agreement is established. Afterwards, the ongoing payment must not be identified as MOTO, but as an MIT.

### 5.11.3 Using a stored credential established by MOTO

A merchant may obtain a cardholder's credential for storage and future use via the MOTO channel. It is important for merchants to understand that any subsequent CITs using a stored credential established over MOTO must be flagged according to the circumstances of the current transaction. For example:

- When a stored credential is established via MOTO, this initial CIT is to be indicated as a MOTO and as MOTO transactions are out of scope of PSD2, SCA is not required.

- Any future CITs initiated using that stored credential must be flagged according to the channel over which that transaction is being performed. For example, if over the phone, the transaction can be flagged as MOTO and is out of scope; if initiated via the merchant website, it must be flagged as eCommerce and SCA, or a suitable exemption is required.
- If the credential is obtained for use in future MITs, refer to Section 5.11.2 above

The fact that a transaction uses a stored credential obtained via MOTO does not mean it can be considered a MOTO transaction for the purposes of SCA. Each transaction which uses stored credentials must be evaluated according to the circumstances of that transaction whether the card details were stored or are entered only for the completion of that transaction is irrelevant to the SCA or no SCA decision.

#### Key Point

Each transaction must be evaluated for its own circumstances. A transaction using credentials obtained via MOTO is not necessarily a MOTO transaction.

#### 5.11.4 Agreements established prior to PSD2 RTS for SCA coming into effect

If a merchant has an agreement in place prior to 14 September 2019<sup>91</sup> for any kind of MIT (standing instructions or industry specific) then the merchant does not need to establish a new agreement with the customer. However, the merchant is required to ensure ongoing payments are submitted in accordance with the MIT Framework for Issuers to recognize those transactions as being out of scope. To do this, the merchant must store the Transaction ID of the payment processed to set up the agreement or one of the payments processed under the agreement and dated prior to 14 September 2019 so that it can be used as the "initial Tran ID" for all future transactions using the MIT Framework. This process is known as "grandfathering". If the merchant does not have any previous Transaction ID available, for an interim period of time, a Visa Acquirer-assigned interim Transaction ID can be used if supported by the Acquirer. Refer to Section 3.10.1.2 for more details.

#### Best Practice

Merchants who intend to use grandfathering as a means of continuing agreements established prior to 14 September 2019 must plan in advance to capture the Transaction ID of the original CIT or a previous MIT to use in future transactions after the 14 September 2019.

<sup>91</sup> As noted in Section 2, NCAs may in some limited cases provide flexibility about their enforcement timescales. This may imply that MITs can be set up without SCA for a period after 14 September 2019, at the discretion of the relevant NCA. References to 14 September 2019 in this section should be read with this qualification.

## 5.12 Changing agreement payment terms

A change to the payment terms of the ongoing agreement sometimes may need to be instigated by either the merchant or the customer. SCA is always recommended in those situations but the merchant may opt not to authenticate if certain conditions apply as described in each scenario.

### 5.12.1 Merchant driven agreement changes

For merchant driven changes to payment terms, authentication is not required provided that the original agreement T&Cs and other cardholder communications clearly cover the eventuality of such changes. If not, SCA is required.

Example changes include:

- The price changes (e.g. due to inflation or other changes for example in the calculation method of the amount)
- The date or frequency of payment changes (e.g. moving from a monthly to yearly billing model)

When a change is made, existing requirements for disclosure and cardholder consent apply, as applicable to the type of agreement.

Note that whether authentication is required or not, the merchant must notify cardholders 7 days before any changes to the agreement, including date of payment or how the amount is calculated. For more information, see Visa Rule ID # 0029844 and 0029267.

### 5.12.2 Customer driven agreement changes

Examples of customer driven changes to payment terms include:

- Changes to pricing or terms, such as
  - Package (e.g. switch from premium to standard or vice versa)
  - Change of billing cycle (e.g. from monthly to yearly)
- Pausing or stopping and then restarting a subscription, such as
  - A subscription is paused by a customer to be restarted at an unknown later date
  - Customer agrees to pause a subscription and resume at a certain date (e.g. "I'm going away for 3 months, please pause my service contract until I return".)
  - Customer explicitly cancelled a subscription, but later returns as a customer

Whether the customer requests a change to pricing and terms or pauses or stops and then restarts an agreement, authentication is not required provided that the agreement T&Cs clearly cover the eventuality of such changes and the merchant has appropriate risk management in place. If there is any doubt that the T&Cs cover the change or if there is a risk of fraud, then the change should be treated in the same way as setting up a new agreement. As there is an existing relationship between the merchant and the customer, merchants with appropriate risk management in place may decide to use the approach to establish a new agreement as described in Section 5.11.

### Key Point

If a customer with an existing agreement requests to change the card used to pay for the agreement, or takes any other remote action with a risk of payment fraud, then this is considered the same as setting up a new agreement.

## 5.13 Executing payments based on established agreements

Once an agreement has been established then the merchant can use that agreement to execute payments, within the T&Cs of that agreement. The following sections give examples of the different types of MIT that a merchant could use, depending on the use case they are looking to deliver.

### Key Point

MITs are out of scope of PSD2 SCA, therefore no SCA is required provided the initial CIT used to set up the agreement has been performed in accordance with Section 5.11. This remains the case for as long as the agreement is in force. There is no time limit after which SCA must be reapplied. If the agreement changes, then in some cases SCA may be required, as outlined in Section 5.12.

### 5.13.1 Installments and prepayments

Installments are payments made in the case where the customer establishes an agreement to pay for goods received in one or more installments over an agreed period. For example:

- A cardholder places an order with an electrical retailer for a TV costing €600. The consumer agrees to a consumer credit agreement requiring them to make an initial payment of €100 on placing the order followed by a series of 5 monthly installment payments of €100.
- Prepayments are payment(s) made towards a future purchase of goods/services. For example:
  - A cardholder orders a piece of furniture and agrees to pay a deposit at time of ordering, with the balance due when the sofa is delivered.

Scenario
Customer agrees Installment plan or prepayment
<ol style="list-style-type: none"> <li><b>Set up new MIT agreement</b> <ul style="list-style-type: none"> <li>The merchant <b>sets up a new agreement</b> in accordance with Section 5.11 and using the Installment/Prepayment MIT type "I" in the authorization request. Note that this could include the taking of an initial payment or deposit.</li> </ul> </li> </ol>
Date of next payment arrives
<ol style="list-style-type: none"> <li><b>Authorize using MIT Framework</b> <ul style="list-style-type: none"> <li>The merchant<sup>92</sup> <b>authorizes</b> at the time interval and for <i>the amount defined in the Installment/prepayment agreement</i>. The transaction must be identified as an Installment/prepayment MIT subsequent transaction (see Table 22). <ul style="list-style-type: none"> <li>The merchant must populate any applicable data in the authorization message as per Section 5.1.2.</li> </ul> </li> </ul> </li> <li><b>Clear funds</b> <ul style="list-style-type: none"> <li>The merchant <b>clears</b> the transaction for the amount based on the <i>Installment/prepayment agreement</i>.</li> </ul> </li> </ol>
Payment schedule complete

For more information on rules applicable to Installments and Prepayments, see Visa Rule ID # 0029267. Key highlights as of January 2019 are as follows:

If the cardholder cancels within the terms of the cancellation policy, the merchant or its agent must provide to the cardholder both of the following within 3 business days<sup>93</sup>:

- Cancellation or refund confirmation in writing
- Credit Transaction Receipt for the amount specified in the cancellation policy

If an Authorization Request for a subsequent payment is declined, the merchant or its agent:

- Must notify the Cardholder in writing and allow the Cardholder at least 7 days to pay by other means.

A merchant or its agent must **not**:

- Process an initial Installment Transaction until the merchandise or services have been provided to the Cardholder
- Process individual Installment Transactions at intervals less than 7 calendar days

<sup>92</sup> It is possible that the merchant processing the Installments with which the customer has an agreement and the retailer providing the goods could be different.

<sup>93</sup> For prepayments, if the Cardholder does not cancel (or pay the remaining balance, if applicable) within the terms of the cancellation policy, the Merchant may retain the prepayment(s) only if the Merchant has disclosed on the Transaction Receipt that the prepayment is non-refundable.

### 5.13.2 Subscriptions at fixed interval

These are payments for the delivery of ongoing goods or services. They have a fixed interval for each payment, but the amount can be fixed or variable, as established in the merchant customer agreement. Examples include:

- Regular payments for a magazine subscription
- Regular payments for an on-demand digital entertainment service
- Monthly mobile phone or utility bill payments
- Quarterly payment for a gym membership

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, as explained in Section 5.11.

Several rules apply to recurring payments. For more information see Visa Rule ID # 0029844 and 0029267. Key highlights as of January 2019 are as follows:

Using the method of communication agreed with the cardholder, the merchant must inform the cardholder of the following:

- Provide the cardholder with confirmation that a Recurring Transaction agreement has been established within 2 business days.
- Provide the fixed dates or regular intervals on which the transactions will be processed (not to exceed one year between transactions)
- Provide notification to the cardholder at least 7 working days before taking payment:
  - In the event of a trial period, introductory offer, or any promotional activity has expired, or
  - If more than six months have elapsed since the previous transaction in the series

At the same time as providing these notifications, the merchant must advise the cardholder how to cancel the agreement with the merchant. A simple cancellation procedure, and, if the cardholder's order was initially accepted online, at least an online cancellation procedure must be available.

A merchant must not complete a recurring MIT:

- Beyond the duration expressly agreed by the cardholder
- If the cardholder requests that the merchant or its agent change the payment method
- If the cardholder cancels according to the agreed cancellation policy
- If the merchant receives a Decline Response

Finally, the following are best practices a merchant should consider implementing:

- Remind the cardholder of the upcoming payment one or two days ahead of the payment even if payment is on a regular or fixed date. This is not only a positive experience for the cardholder but maximize chances of funds being available

- Check the Visa Account Updater (where available) before submitting the transactions. The service provides payment card updates, which means that merchants can avoid declines due to expired cards and other costs and inconveniences associated with re-issued cards
- Take care to ensure that the correct expiry date is included with each transaction. Issuers may choose to decline transactions if it is incorrect or missing.
- Should not submit a recurring transaction through more than one Acquirer unless the names used (line 1 & 2 of the statement narrative and/or MID) are identical
- Should not submit incorrect or misleading authorization data in an attempt to avoid a stop instruction placed against a card

Scenario
Customer signs up for ongoing service or subscription
<b>1. Set up new MIT agreement</b> <ul style="list-style-type: none"> <li>• The merchant <b>sets up a new agreement</b> in accordance with Section 5.11 and using the Recurring MIT type.</li> </ul>
Customer receives regular goods or service
<b>2.</b> Customer receives regular goods (e.g. monthly magazine), or service (e.g. access to on demand video content, mobile phone connectivity).
Agreed payment interval reached
<b>3. Authorize using MIT Framework</b> <ul style="list-style-type: none"> <li>• The merchant must communicate with the cardholder, if required, prior to processing an MIT (refer to Visa Rule ID # 0029844 and 0029267)</li> <li>• The merchant <b>authorizes</b> the amount based on the recurring payment agreement at the pre-agreed interval as a Recurring MIT subsequent transaction (see Table 20).               <ul style="list-style-type: none"> <li>◦ The merchant must populate any applicable data in the authorization message as per Section 5.1.2.</li> </ul> </li> </ul>
<b>4. Clear funds</b> <ul style="list-style-type: none"> <li>• The merchant <b>clears</b> the transaction for the amount based on the recurring payment agreement.</li> </ul>
Customer ends agreement

### 5.13.3 Signing up for services charged at irregular intervals (usage based)

This is the type of agreement where the amount and/or the time period between payments is variable and cannot be defined at time of agreement. Payment is usually triggered based on usage. For example, a customer might sign up for:

- Top-up for a prepaid account when balance reaches a pre-agreed level (e.g. mobile phone or Mass Transit).
- An ongoing delivery agreement for a service such as groceries (e.g. reserving a weekly time slot for delivery of groceries with the facility that the time slot may be



changed or cancelled, and items can be added to basket until a pre-agreed cut off time).

- A bike or car share scheme where payment is made based on usage.
- Transport services such as usage of a transponder or other device for road tolling or unattended parking where payment is made based on usage.
- Receipt of a "basket of goods" on a regular basis from which the customer decides which items to keep and returns unwanted goods. The merchant charges upon receipt of unwanted items or after an agreed time period, whichever comes first, for the items not returned.
- A snow clearance service where the driveway of a customer is cleared by the merchant after each snowstorm in the winter months.
- Aggregated payments using a stored payment credential (e.g. purchases from a mobile app store)

This can only be treated as an MIT where the cardholder is not directly engaging with the merchant, in a manner which allows authentication to take place.

Several rules apply to Unscheduled Credential on File payments. For more information see Visa Rule ID # 0029844 and 0029267. Key highlights as of January 2019 are as follows:

- Using the method of communication agreed with the cardholder, a merchant must provide notification to the Cardholder of any change in the agreement, including, but not limited to, any change in the way the amount of the transaction may be calculated, at least 2 working days before the change.
- A simple cancellation procedure, and, if the cardholder's order was initially accepted online, at least an online cancellation procedure must be available.

A merchant must not complete a recurring MIT:

- Beyond the duration expressly agreed by the Cardholder
- If the Cardholder requests that the merchant or its agent change the payment method
- If the Cardholder cancels according to the agreed cancellation policy
- If the merchant receives a Decline Response

Finally, the following are best practices a merchant should consider implementing:

- Check the Visa Account Updater (where available) on a regular basis. The service provides payment card updates, which means that merchants can avoid declines due to expired cards and other costs and inconveniences associated with re-issued cards
- Take care to ensure that the correct expiry date is included with each transaction Issuers may choose to decline transactions if it is incorrect or missing
- Should not submit a recurring transaction through more than one Acquirer unless the name used (line 1 & 2 of the statement narrative and/or MID) are identical
- Should not submit incorrect or misleading authorization data in an attempt to avoid a stop instruction placed against a card

Scenario	
Customer and merchant establish agreement	
1. <b>Set up new MIT agreement</b>	<ul style="list-style-type: none"> <li>The merchant <b>sets up a new agreement</b> in accordance with the options in Section 5.11 and using the UCOF MIT type.</li> </ul>
Customer consumes goods or service	
2.	The customer receives goods or consumes service at any time. No further authentication or authorization is required.
Merchant ready to request payment	
3. <b>Authorize using MIT Framework</b>	<ul style="list-style-type: none"> <li>The merchant must communicate with the cardholder, if required, prior to processing an MIT (refer to Visa Rule ID # 0029844 and 0029267)</li> <li>The merchant <b>authorizes</b> an amount based on the agreed method of calculation in the agreement as a UCOF MIT subsequent transaction (see Table 22). <ul style="list-style-type: none"> <li>The merchant must populate any applicable data in the authorization message as per Section 5.1.2.</li> </ul> </li> </ul>
4. <b>Clear funds</b>	<ul style="list-style-type: none"> <li>The merchant <b>clears</b> the transaction for the amount based on the agreed method of calculation in the agreement.</li> </ul>

#### 5.13.4 Processing a purchase at the same time as establishing a new agreement

In this scenario, a merchant may give a customer the option to sign up for a Standing Instruction (recurring, installment or UCOF) at the same time as making another purchase. For example, a customer could:

- Purchase a phone and at the same time sign up for a monthly data plan
- Purchase a DVD and also sign up for ongoing streaming payable monthly
- Buy a book and sign up for weekly paper or digital magazine at the same time
- Purchase a mobile phone and a care agreement for that phone
- Booking a holiday trip and subscribing to a travel membership scheme paid on a monthly basis<sup>94</sup>

<sup>94</sup> For all travel-related scenarios, please also refer to the Visa Guide: *Implementing Strong Customer Authentication (SCA) for Travel & Hospitality*

## Scenario

### Customer checks out and agrees to ongoing payments

#### 1. Authenticate customer

- The merchant **authenticates** the transaction immediately for the amount due that day (total for purchase and agreement), obtaining a CAVV for later submission in the authorization.
- As the establishment of an agreement requires explicit cardholder authentication, exemptions cannot be exercised in most cases (refer to Section 3.10 for the cases where exemptions can be applied).

#### 2. The merchant can choose one of the following options:

(a) Perform a single **authorization** for the full amount due that day

(b) Perform two separate **authorizations** for purchase amount and agreement amount respectively

- In case of **option (a)**, the merchant performs a single **authorization** for the full amount due that day, and populates any applicable authentication-related data in the authorization message as per Section 5.1.1
  - This authorization must be flagged as the initial CIT for enabling subsequent MITs (see Table 22).
  - The Transaction ID of this authorization must be stored for usage in the future MITs.
  - The receipt for this transaction must fulfil all obligations for both the agreement and the purchase.
  - It is recommended that the transaction be cleared as a single amount but with the receipt clearly breaking down into the amount charged for the purchase and the amount for the agreement to avoid customer confusion.
- In case of **option (b)**, the merchant performs two separate **authorizations** in succession and **clears** two transactions as below:
  - An authorization for the purchase.** The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1.
    - As this transaction is not being used to establish the agreement, any applicable exemptions can be exercised.
  - An authorization for the amount due today related to the agreement.** The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1.
    - As the establishment of an agreement requires explicit cardholder authentication, exemptions cannot be exercised in most cases.
    - This authorization must be flagged as the initial CIT for enabling subsequent MITs of the appropriate type (see Table 22).
    - The Transaction ID of this authorization must be stored for usage in the future MITs.
    - The CAVV and associated ECI value must also be submitted with this transaction as proof of authentication if required for the agreement.

### Customer uses service

#### 3. Authorize using MIT Framework

- The merchant must communicate with the cardholder, if required, prior to processing an MIT (refer to Visa Rule ID # 0029844 and 0029267)
- The merchant **authorizes** future MITs, identified as detailed in (see Table 22).
  - The merchant must populate any applicable data in the authorization message as per Section 5.1.2.
- The amount in future MITs may vary from the original amount as long as the amount calculation method is disclosed to the customer in the T&Cs of the established agreement.
- The merchant performing the MIT could be different to the merchant that performed the CIT, provided the conditions outlined in Section 5.16.1 are met.

#### 4. Clear funds

- The merchant **clears** the transaction for the amount in the MIT.

## 5.14 Visa Direct payment

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.

Transactions associated with the Visa Direct service fall into two categories:

1. Original Credit Transactions OCTs; used to “push” funds to a Visa cardholder’s account
2. Account Funding Transactions (AFTs); used to “pull” funds from a Visa cardholder’s account

Refer to Section 4.8 for definitions of these transaction types and guidance on when SCA is and is not required.

### 5.14.1 Example Visa Direct use cases and use of OCTs and AFTs

Table 39 summarizes examples of push payment services that are supported by Visa Direct, indicating whether an AFT and/or OCT is used:

**Table 39: Example use cases showing usage of AFT and OCT**

Example	Description	AFT	OCT
Peer-to-Peer (P2P) money transfer	Customer (A) sends money from their payment card to be credited to the payment card of customer (B), via a payment service.	Yes	Yes
Prepaid load	Customer (A) loads money into a prepaid card, e-money or stored value account held by a third-party financial institution using their Visa payment card as a funding source	Yes	No
Funds disbursement	General, business and government-initiated funds disbursements including for example: <ul style="list-style-type: none"><li>• Reimbursements</li><li>• Refunds</li><li>• Rebates</li><li>• Pay-outs</li><li>• Loan distributions</li><li>• Government disbursements</li></ul>	No	Yes

### 5.14.2 OCTs and SCA

OCTs are identified by Field Value 26 in Authorization Field 3.

OCTs do not require SCA to be performed on the recipient of the funds. Therefore, an Issuer may not use Response Code 1A (SCA required) in response to authorization requests properly identified as OCTs.

These transactions should be flagged by transaction originators using code value 26 in Field 3.

Issuers can identify an OCT by checking for the processing code value of 26 in Field 3.

### 5.14.3 AFTs and SCA

AFTs are identified by Field Value 10 in Authorization Field 3.

AFTs are processed as e-commerce transactions and therefore the 3DS and Authorization flags and flows, as well as the tools and services (such as Visa Trusted Listing and the Visa MIT Framework) described in Section 3 apply to AFT transactions in the same way as other remote electronic transactions. This is true whether the transactions originated through ISO messages or via the Visa Direct AFT API.

As per Section 4.8.3 AFT transactions are in scope of PSD2 SCA and therefore authentication must be performed, or a suitable exemption exercised. For example, if the AFT is a single transaction of a known amount to fund a one-time payment, the process described for a one-time purchase in Section 5.2 should be followed, but with the additional inclusion of the value 10 in Field 3.

## 5.15 B2B payments

### 5.15.1 Introduction: The secure corporate payment processes and protocols exemption

Under SCA-RTS Article 17, PSPs are allowed not to apply strong customer authentication for payments made by payers who are 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 and other relevant requirements are met. This is through application of the secure corporate payment processes and protocols exemption defined in Article 17 of the SCA RTS.

Subject to local regulatory interpretation, the exemption may be applied to card payments in certain circumstances, notably:

- Where the card product being used is recognized by the NCA as qualifying as a secure payment process or protocol in its own right – for example a virtual card or a lodged card that is not issued to an individual
- Where the card is a physical commercial card issued to an individual named employee and the payment is initiated within a secure, access-controlled corporate purchasing system

Note the exemption cannot be applied to:

- Commercial cards used in a non-secure environment – for example to purchase goods or services from a supplier's public website
- Consumer cards, even if they are used within a secure corporate environment

For more guidance on interpreting the exemption, how it applies in the context of different card product types (physical commercial cards, virtual cards, lodge cards and consumer cards) and what may constitute a secure process or protocol please refer to Section 4.5.4.

### 5.15.2 Circumstances under which the exemption may be applied

The secure corporate payments exemption can only be applied by commercial card Issuers, however there are two distinct circumstances determining how it is applied:

- 1) Where the Issuer is able to identify that the transaction qualifies for the exemption – for example through identifying that the transaction is being made using a recognized qualifying product – for example a virtual card.
- 2) Where the merchant or Acquirer is able to indicate to the Issuer that the payment is being initiated using a secure process or protocol – for example a physical card used within a secure corporate procurement system or process.

### 5.15.3 The Secure Corporate Payment Indicator

Visa has made available a Secure Corporate Payment indicator in TLV Field 34 (Tag 88 in Dataset ID 4A) to enable a merchant or Acquirer to indicate that they would like the secure corporate payment exemption to be applied. The indicator is provided to help the Issuer make a decision about whether to apply the exemption. This is particularly important in cases where a commercial product could also be used outside of secure corporate environments (a physical commercial card issued to a named cardholder).

### 5.15.4 Practical Guidelines on applying the exemption: Transactions using Commercial Cards not issued to individuals

#### 5.15.4.1 Merchant Guidelines: Commercial cards not issued to individuals

Many commercial card products do not have an individual cardholder associated with them, and as such there is no cardholder to be authenticated at the time of a transaction. Transactions with such card products, specifically virtual cards and lodged cards, only originate from a secure corporate environment.

The way in which a Merchant assesses and routes a transaction will depend on whether or not the merchant is aware at the time of transaction that such a product is being used:

- If the merchant is not aware, it must assess the transaction in the same way as any other. It may choose to either:
  - Submit the transaction to authorization requesting another exemption, or
  - Submit the transaction to 3DS for authentication.

If the transaction is submitted to 3DS there are two possible outcomes:

1. If the Issuer of the commercial card has enrolled the PAN into 3DS, in which case, the transaction will be directed to the Issuer's ACS. This will enable the Issuer to apply the secure corporate payment exemption and return an ECI 05 and a CAVV for authenticated transaction to enable the authorization to proceed. If the request does not satisfy the secure corporate card exemption, the Issuer may proceed with a challenge to authenticate the cardholder.
  2. If the Issuer of the commercial card has not enrolled the PAN into 3DS then the transaction will be directed to the Visa Attempts Server. Visa will return an ECI 06 and associated CAVV to the merchant, enabling the authorization to proceed.
- If the merchant is aware and therefore knows the transaction qualifies for the secure corporate payment exemption, it can choose to send the transaction straight to authorization. Issuers are asked to recognize the transaction as qualifying for the secure corporate payment exemption according to how they have segmented these products in their systems. This also means that it is not essential to populate the Secure Corporate

Payment Indicator in F34 of the transaction (subject to this being approved by the relevant NCA). If, however a merchant is able to update their systems to apply the Indicator, this is recommended. Merchants should discuss this with their Acquirer.

#### 5.15.4.2 Issuer Guidelines: Commercial cards not issued to individuals

Issuers that receive authorization requests without authentication data relating to a product that is not issued to an individual and is only used within a secure corporate environment (for example virtual cards and lodged cards) should apply the secure corporate payment exemption (where approved by the relevant NCA) and should not request SCA, even if the Acquirer has not populated the Secure Corporate Payment indicator.

Such transactions can only originate from a secure corporate environment and should be identifiable by the Issuer according to how they have segmented or flagged their PANs for these products<sup>95</sup>.

When such cards are used at merchants that are not aware that the card has no individual cardholder, the merchant may submit the transaction to 3DS. Therefore, it is recommended that Issuers of these cards enroll the PANs in 3DS and ensure that they have in place suitable rules at their ACS to allow such transactions to proceed under the secure corporate payment exemption, should they be received.

### 5.15.5 Practical Guidelines on applying the exemption: Transactions using Commercial Cards issued to individuals

#### 5.15.5.1 Merchant Guidelines: Commercial cards issued to individuals

Some commercial card products involve the issuance of plastic cards to individual employees. When such cards are used in a secure corporate environment (for example, if the details are also held in a corporate purchasing system that meets the criteria required by the relevant NCA) then the secure corporate payment exemption may be applicable.

In this case, it is important for merchants and Acquirers to note that because the product can be used for business expenditure in both public and corporate environments, the Issuer will not be able to identify that the exemption can be applied unless the Secure Corporate Payment indicator has been populated.

The guidelines provided elsewhere in this guide should be followed for any type of transaction made by individuals in a public environment using physical commercial cards held in their possession. In these circumstances the secure corporate payment exemption is not applicable.

#### 5.15.5.2 Issuer Guidelines: Commercial cards issued to individuals

When making authorization decisions for commercial cards issued to individuals, Issuers should consider that when the Acquirer has indicated that the transaction originates from a secure corporate environment, it is generally not possible to authenticate an individual payer at the time of the transaction and as such, they should not request SCA on transactions where the Secure Corporate Payment indicator is populated.

---

<sup>95</sup> Visa Rule #0026398 states "All Visa Central Travel Accounts must be distinguished from other Visa Commercial Cards issued on the same BIN". Issuers complying with these rules should be able to identify transactions using such products and will be able to apply the Secure Corporate Payment exemption.

#### 5.15.6 Example B2B Payment Use Cases

The following are examples of B2B use cases where the secure corporate payment exemption may be applicable:

- A commercial card product whose details are lodged with a trusted corporate supplier and used purely for secure corporate purchase transactions with that supplier
- A commercial card product whose details are securely lodged with a dedicated business to business marketplace (i.e. not a public internet website)
- A commercial card product lodged or embedded within a secure corporate procurement system for making purchases from approved suppliers

Additional use cases specific to the travel and hospitality industry are described in the Travel and Hospitality Addendum to this Guide.



## 5.16 Multi-party commerce

Depending on the scenario, customer interactions could have one or more than one merchant.

### 5.16.1 Multiple merchants

A merchant setting up an agreement may not be the same as the merchant processing subsequent MITs. For example, a customer could:

- Buy a fridge from a white goods supplier, but the installments could be collected by a third party credit provider.
- Purchase both a mobile phone and a care contract for the phone in-store. The care contract is fulfilled by a third party provider.
- Purchase furniture in-store and pay for delivery and installation by a third party contractor

#### Key Point

The merchant performing the initial CIT and the merchant collecting subsequent MITs can be different, as long as the customer is clearly informed. This means that the Initial Tran ID in an MIT transaction may be related to a CIT transaction that was performed by a different merchant and a different Acquirer.

Therefore, the Visa authorization system allows the CIT and MIT to originate from different merchants (i.e. merchant descriptor and merchant ID can be different), and different Acquirers as long as:

- The customer has been clearly informed who he or she is transacting with at the time of CIT and which merchant he or she is authorizing to perform MITs in the future. (e.g. T&Cs and other clear communication inform the customer that the merchant name will differ from the initial transaction to the subsequent transactions);
- There is a way to prove the relationship between the two merchants (e.g. T&Cs presented to cardholder show who is taking payment today and who is taking payment in the future etc.)

It is important for merchants working together to be aware that whilst it is acceptable for merchants to set up agreements for each other (provided it is clear covered in T&Cs) it is not acceptable for any merchant to collect funds on behalf of other merchants for their goods and services unless they do so under a Visa recognized payment model such as Payment Facilitator or Marketplace as defined below.

### 5.16.2 Marketplaces (single merchant)

As per Visa rule ID# 0030069, Visa defines online marketplaces to be environments where a single entity brings together buyers & sellers on a branded platform and collects payments on behalf of the other parties who provide goods or services to the customer under the marketplace brand. The marketplace owns the overall customer relationship, is responsible for the transactions and often sets T&Cs of the sale. Examples could include:

- An online marketplace for goods where the payment is always taken by the marketplace operator.

- A take-away food delivery company, where the payment is always taken by the delivery company, and not the establishment providing the food.

A Marketplace must:

- Ensure that its name or brand is:
  - Displayed prominently on the website or mobile application
  - Displayed more prominently than the name and brands of retailers using the Marketplace
  - Part of the mobile application name or URL
- Handle payments for sales and refunds on behalf of the retailers that sell goods and services through the Marketplace, and receive settlement for transactions on their behalf
- Be financially liable for disputes and resolve disputes between cardholders and retailers

In these cases, the merchant will be the same across all aspects of service delivery (i.e. the Marketplace brand), even if different parties are involved in aspects of the fulfilment.

From an SCA perspective, it is the Marketplace brand that will be responsible for authentication and authorization. The name of the merchant providing the goods or services is not seen anywhere in the Visa system, neither in the authentication nor authorization.

**IMPORTANT:** An entity that brings customers and merchants together but does not handle payments on behalf of the merchant is not considered a Marketplace under Visa Rules but a referral service. For more information see Section 5.16.4.

### 5.16.3 Payment Facilitators

Payment Facilitators are parties that authorize and settle on behalf of a merchant, but it is the merchant that provides the goods and services and has the relationship with the cardholder.

From an SCA perspective, it is the merchant that drives requests for authentication and authorization, however many merchants using Payment Facilitators may not have the capability or desire to do this in-house, and so it is anticipated they will use services provided by their Payment Facilitator or another technology/gateway provider.

For more details on requirements for transactions with Payment Facilitators, please refer to Visa rule ID #: 0030076.

### 5.16.4 Referral services

A referral service is a website that brings customers and merchants together, but unlike a Marketplace, the referral service does not handle payments on the merchant's (i.e. seller's) behalf. The payment between the buyer & seller occurs through a separate, unrelated channel from that of the original website.

For example:

- A website that dog owners use to find local dog walkers and compare location and prices
- A website that brings together people needing care in the community with different care agencies

- A classifieds website for individuals to list personal items or services for sale
- A website that brings together many artists selling their own products directly

From an SCA perspective, it is the merchant (i.e. the actual seller of goods/services) that drives requests for authentication and authorization, not the referral service. The referral service is not involved in any way in the payment and authentication process. The end merchant could implement their processes themselves or use a Payment Facilitator.

If the referral service wished to expand their service offering, they could consider offering authentication and authorization services to their merchants, but this would require them successfully undertaking all the processes required to register with Visa as a third party agent. In such cases, they would have to perform a separate authentication for each merchant (via each merchant's Acquirer) involved in a customer order. It is not permissible for a service that does not handle payments to perform a single authentication and then provide the authentication data to multiple merchants with the exception of Travel Agencies (MCC 4722<sup>96</sup>).

Alternatively, a Referral Service wishing to provide authentication services to multiple merchants could enhance their offering to become a qualified & registered Marketplace and aggregate all the payments for their suppliers/retailers, thus enabling them to perform a single authentication for a basket containing goods from multiple merchants.

### 5.17 Industry Specific Best Practice

Industry Specific Best Practice MITs are primarily relevant to the Travel and Hospitality sector. This sector handles many types of payment including:

- No Show at a hotel or car rental agency
- Delayed Charges at a hotel or card rental agency
- Other additional charges such as for an additional night stay, mini bar charges in hotel
- Balance payment(s) on purchase or service on which a deposit has been paid

Further detail on how these industry specific scenarios should be processed are provided in an addendum to this guide titled *"Implementing Strong Customer Authentication for Travel and Hospitality"*.

---

<sup>96</sup> Please refer to the Visa Guide *Implementing Strong Customer Authentication (SCA) for Travel & Hospitality* for more information on how Travel Agents can do this.

## 5.18 Non-financial scenarios

This section covers some example ecommerce scenarios for non-financial transactions. In some circumstances, SCA should still be performed when considering the non-financial transaction in the context of any financial transactions that might follow.

### 5.18.1 Adding a card to a merchant account/customer profile

This describes the use case when a customer requests addition of a card to a merchant account for future customer-initiated purchases only, but no financial transaction is performed at time of addition. For example, the customer is setting up payment details for a new account.

In this scenario, the payment details must be stored in accordance with the Stored Credential Framework:

Scenario
Customer logs on to merchant and adds a payment credentials to their account
<ol style="list-style-type: none"><li><b>1. Disclose use of stored credential</b><ul style="list-style-type: none"><li>The merchant must <b>disclose</b> to the customer how the stored credential will be used.</li><li>For more information about the Stored Credential Framework and the requirements a merchant must meet, see Appendix A.4.</li></ul></li><li><b>2. Obtain cardholder consent</b><ul style="list-style-type: none"><li>The merchant must <b>obtain</b> cardholder consent. Refer to same Appendix A.4 for more information.</li></ul></li><li><b>3. Authenticate customer, if risk of fraud</b><ul style="list-style-type: none"><li>SCA is required if there is a risk of fraud. A merchant may submit a non-payment <b>authentication</b> request to 3DS to confirm the customer's identity. This does not provide fraud liability protection.</li></ul></li><li><b>4. Perform a zero-value <i>account verification</i></b><ul style="list-style-type: none"><li>Merchant must perform a zero-value authorization (account verification), using indicators according to the Stored Credential Framework, to inform the Issuer that the credential is being stored (and incidentally verify the validity of the credential).</li><li>Note: If a new card is added, go back to step 1</li></ul></li></ol>
Customer makes future payment using stored credential
<ol style="list-style-type: none"><li>Future CITs using the stored credential must be <b>authenticated</b> unless a valid exemption applies.</li></ol>

When using a stored credential, a merchant must comply with the relevant disclosure, consent, cancellation procedure and processing rules (see Visa Rule ID # 0029267).

### 5.18.2 Adding a card to an account during a purchase

A customer requests the addition of a Credential-on-File for future use with the merchant during a purchase transaction.

Scenario
Customer agrees to add payment credentials to their account as part of a purchase
<ol style="list-style-type: none"><li><b>1. Disclose use of stored credential</b><ul style="list-style-type: none"><li>• Merchant must <b>disclose</b> to the customer how the stored credential will be used.</li><li>• For more information about the Stored Credential Framework and the requirements a merchant must meet, see Appendix A.4: Stored Credential Framework.</li></ul></li><li><b>2. Obtain cardholder consent</b><ul style="list-style-type: none"><li>• Merchant must <b>obtain</b> cardholder consent.</li></ul></li><li><b>3. Authenticate customer</b><ul style="list-style-type: none"><li>• As this is a financial transaction, <b>authentication</b> is required for the amount of the financial transaction unless an exemption applies. However, adding the card may require SCA if there is a risk of fraud in which case exemptions cannot be used.</li></ul></li><li><b>4. Authorize transaction</b><ul style="list-style-type: none"><li>• Merchant submits an <b>authorization</b> for the transaction amount and includes the appropriate identifier to indicate that a card is being stored according to the SCF (refer to Appendix A4 – Stored Credential Framework for more details on this indicator).<ul style="list-style-type: none"><li>◦ The merchant must populate any applicable authentication-related data in the authorization message as per Section 5.1.1</li></ul></li><li>• Merchants must be aware that if the transaction is declined, the credentials cannot be stored.</li></ul></li></ol>
Customer makes future payment using stored credential
<ol style="list-style-type: none"><li><b>5. Future CITs using the stored credential must be <b>authenticated</b> unless a valid exemption applies. They must also be indicated with POS entry mode 10 (stored credentials).</b></li></ol>

### 5.18.3 Adding a card at the same time as setting up an agreement

A customer requests the addition of a Credential-on-File for future use with the merchant at the same time as establishing an agreement for MITs.

This option for merchants has already been covered as part of the new agreement scenario descriptions in Section 5.11.

### 5.18.4 Card details updated by the Issuer

Merchants storing credentials can receive updated payment credentials from the Issuer (e.g. via Visa Account Updater (VAU) or the Visa Token Service). Examples of events that could cause this include:

- Regular card re-issuance due to expiry date being reached, and
- An Issuer switching their card portfolio from another card scheme to Visa

Whilst authentication is not required, it is Visa's recommended practice that merchants using a cardholder's stored credential who receive updates on account information from Visa inform customers in their T&Cs and/or privacy policy that the card details may be automatically

updated by participating Issuers in order to ensure payment continuity and uninterrupted service.

#### 5.18.5 Cardholder switching Issuers under the UK Current Account Switch Service

It is possible for a Cardholder to switch their current account (and any associated Visa payment cards) from one Issuer to another. Proof of consent from the Cardholder must be obtained to perform the switch. In the UK Visa Account Updater supports the current account switching service as follows:

- The bank the customer has switched to will send an update to Visa Account Updater to indicate that the old account has been replaced because of an account switch along with a new account number
- The bank the customer is leaving will send an update to Visa Account Updater to indicate that the old account has been closed because of an account switch

Merchants storing details of payment cards can query Visa Account Updater to ensure they have up-to-date information. A merchant who becomes aware of an account switch by querying Visa Account Updater is not required to perform additional cardholder authentication before updating their records with the new account details. However, it is Visa's recommended practice that merchants who update a cardholder's stored credential based on account information from Visa Account Updater inform customers in their T&Cs and/or privacy policy that the card details may be automatically updated by participating Issuers in order to ensure payment continuity and uninterrupted service.

#### 5.18.6 Card details updated by the Customer

If a cardholder goes into their merchant account and updates their card details, either because they wish to pay via a new card, or because the old card had expired, SCA is required if there is a risk of fraud.

If only the expiry date is changed and the card number remains the same, authentication is not required.

#### 5.18.7 Change Delivery Address

If a cardholder goes into their merchant account and updates the delivery address for an order, authentication is not required, but Visa recommends that it is performed if the customer changes the delivery address linked to an order that is already being processed as this represents a risk of fraud.

### 5.19 Provisioning Network Tokens

Merchants that use Visa Token Service (VTS) to provision tokens for eCommerce and Credential-on-File (CoF) transactions should refer to the VTS Implementation Guide for details of how to ensure tokens are provisioned correctly. In the context of establishing agreements for ongoing payments such as subscriptions, please refer to Section 5.11.

### 5.20 Mass tokenizing existing credential on file

For bulk tokenization, SCA is not required as this is just changing the format of a credential already held on file based on an existing agreement which can continue without having to re-authenticate.

## 6. Planning for PSD2 – what you need to do

Visa clients, merchants and other stakeholders need to plan and prepare for the enforcement of PSD2.

This section summarizes the key decisions and actions that need to be taken by each stakeholder group and identifies the sections of the guide that provide more detailed guidance:

### 6.1 Issuer planning checklist



Issuers should ensure they have a PSD2-SCA plan in place that covers at least the following critical decisions and actions:

**Table 40: Issuer planning checklist**

1 Ensure you have the latest technology in place to optimize for PSD2		
1.1	Plan to migrate to EMV 3DS 2.2.0 as early as possible.	<ul style="list-style-type: none"><li>• Visa expects all Issuers to support EMV 3DS 2.1.0 by 14 March 2020 and to support EMV 3DS 2.2.0 by 14 September 2020. See Section 3.3.2 for more information.</li><li>• Consult your ACS vendor to agree a migration schedule</li><li>• Visa is able to offer an ACS capability to Issuers whose ACS vendor is unable to migrate them within an acceptable timescale</li></ul>
1.2	Ensure you can still support legacy 3DS 1.0	<ul style="list-style-type: none"><li>• Many merchants around the world will still be on 3DS 1.0. It is important to ensure you still support this version for the foreseeable future.</li></ul>
1.3	Plan to adopt RBA as early as possible.	<ul style="list-style-type: none"><li>• All Issuers that do not yet support RBA should consult their ACS vendor to agree on an implementation plan.</li><li>• Any Issuer whose ACS is unable to offer RBA should consider alternative providers</li><li>• Visa is able to offer Issuers additional risk management guidance and RBA services. Consult your Account Executive for more information</li></ul>
1.4	Develop an SCA roadmap	<ul style="list-style-type: none"><li>• Plan to support and migrate to SCA challenge methods that:<ul style="list-style-type: none"><li>• Deliver the simplest user experience</li></ul></li></ul>

		<ul style="list-style-type: none"> <li>Minimize checkout friction</li> <li>Minimize security vulnerabilities</li> <li>Allow consumers to authenticate using technology they can access without reliance on mobile network coverage</li> <li>Note Issuers may need to support more than one method to ensure full inclusivity</li> </ul>
1.5	Develop an SMS OTP Migration Plan	<ul style="list-style-type: none"> <li>Issuers that use or plan to use SMS OTP as an SCA method should liaise with local regulators to agree an implementation plan that includes the use of SMS OTP with card credentials for an interim period, if required. If use of SMS OTP with card credentials is permissible as an interim the Issuer should develop a plan to ensure that it is implemented effectively. This will include: <ul style="list-style-type: none"> <li>Designing the challenge experience to minimize friction</li> <li>Collection of user mobile numbers</li> <li>Mitigation of security risks associated with the use of SMS</li> <li>Development of a customer and stakeholder communications plan</li> <li>Development of an inclusion and fall back strategy for those customers who are unwilling or unable to utilize SMS OTP</li> <li>A migration strategy to adoption of behavioral biometrics as an inherence factor to provide long term compliance</li> </ul> </li> </ul>
1.7	Develop a plan to offer a biometric authentication capability by April 2020.	<ul style="list-style-type: none"> <li>Consult your ACS or authentication vendor to develop a plan to adopt a biometric solution</li> <li>Visa is also able to offer biometric solutions. See Section 3.11 and consult your Visa Account Executive for more information</li> </ul>
1.8	Provide accessibility options	<ul style="list-style-type: none"> <li>Ensure options are available to consumers who cannot or do not wish to use smartphones or other mobile devices</li> <li>Ensure you can support multiple communication channels to your cardholders, such as Wi-Fi, mobile and email, to minimize abandonment and disruption of service</li> </ul>
1.9	Connect with your providers	<ul style="list-style-type: none"> <li>Ensure you are aligned with your ACS provider on your authentication strategy and customization</li> <li>Review whether your current ACS solution will continue to provide you with the optimum solution for the effective application of SCA in the long term.</li> <li>Visa can provide advice to Issuers on ACS upgrades and can offer the VCAS ACS solution. Contact your</li> </ul>



		<p>Visa Account executive of you would like to discuss the options.</p> <ul style="list-style-type: none"> <li>• Ensure your processor will support the new PSD2 fields in the authorization message (see Section 3.2.2 for more information)</li> <li>• Ensure your down-stream systems (e.g. fraud and monitoring) can support the new data elements</li> </ul>
1.10	See how Visa can help you	<ul style="list-style-type: none"> <li>• Visa has solutions that can help you optimize to get you moving quickly (e.g. Visa Advanced Authorization and Visa Risk Manager, Visa Trusted Listing, Visa Delegated Authentication, Visa Transaction Advisor, Visa Consumer Authentication Service (VCAS)). See Section 3 for more details.</li> <li>• Visa will be releasing additional details in the guides, webinars, roadshows, etc. to support you</li> </ul>
<b>2 Develop authentication and authorization strategies &amp; policies</b>		
2.1	Get up to speed	<ul style="list-style-type: none"> <li>• Many transactions may not require Strong Customer Authentication.</li> <li>• So as not to unnecessarily disrupt the customer experience, familiarize yourself with your eligibility for exemptions, the out of scope criteria, and your NCA's guidance on the regulation.</li> </ul>
2.2	Develop overall policies and systems for application of exemptions	<ul style="list-style-type: none"> <li>• Develop risk management and exemption prioritization policies that will minimize the application of SCA challenges for low risk transactions submitted to you for authentication, while maintaining fraud rates within target reference fraud rates and ensuring compliance with Visa Rules on transaction abandonment. For more guidance see Section 4.</li> </ul>
2.3	Develop risk policies to optimize application of the TRA exemption	<ul style="list-style-type: none"> <li>• Define the reference fraud rate band(s) which you intend to comply with in order to apply the exemption</li> <li>• Analyze your fraud and risk management data to identify transaction profiles/risk scores for which the exemption can be applied while maintaining fraud rate below the target reference fraud rate threshold</li> <li>• Work with your ACS vendor to configure your RBA engine</li> <li>• Monitor the effectiveness of your TRA exemption policy in terms of: <ul style="list-style-type: none"> <li>• Measured fraud rate</li> <li>• Latency</li> <li>• Transaction abandonment</li> </ul> </li> </ul>

		<ul style="list-style-type: none"> <li>Ensure you are meeting the fraud reporting and notification guidelines published by your NCA.</li> </ul>
2.4	<p>Develop policies for selecting merchants that will qualify for the trusted beneficiaries exemption and evaluate solutions to implement trusted beneficiaries listing.</p> <p>Note: Issuers may choose not to support the trusted beneficiaries exemption.</p>	<ul style="list-style-type: none"> <li>The trusted beneficiaries exemption will be beneficial for low risk/fraud merchants who are prepared to accept fraud liability under the Visa Rules.</li> <li>It is recommended that Issuers develop a list of merchants who may be listed as trusted beneficiaries based on these criteria.</li> <li>For more information on Visa's Trusted Listing solution please see Section 3.6 and consult your Visa Account Executive.</li> </ul>
2.5	Create your authorization logic and strategy	<ul style="list-style-type: none"> <li>There will be many transactions that will come in without a cryptogram and exemption (notably, out of scope transactions including MITs and one-leg out transactions). If you see this: <ul style="list-style-type: none"> <li>First check to see if the transaction is out of scope of the regulation. If this is the case, follow normal authorization processing. (Note: do not use any SCA response codes.)</li> <li>Use and accept exemptions whenever possible. Your risk-based model will help you identify low risk transactions.</li> </ul> </li> <li>Note: If you receive an authorization without a cryptogram or an exemption request: <ul style="list-style-type: none"> <li>First check to see if an exemption is applicable using a risk-based model such as Visa Advanced Authorization (e.g. low risk, low value) and apply that during the authorization.</li> </ul> </li> <li>If it doesn't, consider responding with a response code 1A (SCA required) requesting Resubmission for authentication. (note: this should only be the case for a small number of transactions).</li> <li>For more information see Sections 4.2 and 4.6.</li> </ul>
2.6	Develop policies and logic for responding to 3RI requests	<ul style="list-style-type: none"> <li>3RI is a 3-D Secure transaction initiated by the 3DS Requestor for the purposes of confirming that an account is still valid or for Cardholder authentication. It can be used to enable merchants to effectively manage some complex use cases.</li> <li>Issuers will need to develop policies for providing authentication data in response to a 3RI request. For more information please refer to sections 3.3.4.1 4.2.4 (Table 27 principle 3), 4.6.3 and 4.6.4.4.</li> </ul>

2.6	Develop policies for handling transactions from merchants that are not prepared for PSD2	<ul style="list-style-type: none"> <li>• It is anticipated that not all merchants will be ready for PSD2 by September 2019</li> <li>• Issuers should develop policies for assessing and taking authorization decisions on transactions that are not submitted for authentication and do not include appropriate exemption or out of scope indicators in the authorization request</li> <li>• Refer to Section 4.6.5 for more information.</li> </ul>
<b>3 Migration Planning &amp; Reporting</b>		
3.1	Ensure migration plans are in place that meet the requirements defined by the EBA and NCAs.	<ul style="list-style-type: none"> <li>• In an opinion published by the EBA on 21 June 2019 the EBA has recognized that NCAs may allow time for all parties in the payments ecosystem to fully implement SCA. This supervisory flexibility was made available under the condition that PSPs set up migration plans, agree their plan with their NCA, and execute the plan in an expedited manner.</li> <li>• A further opinion published by the EBA on 16 October 2019 has set the deadline by which the period of supervisory flexibility should end, and PSP migration plans should be complete as 31 December 2020. This opinion also sets out various requirements on PSPs to provide information and reporting to NCAs and provide information to customers.</li> <li>• Issuers must ensure that migration plans are in place that meet these requirements and should align with migration roadmaps that may be required by NCAs or agreed between industry representatives and NCAs in individual markets.</li> </ul>
3.2	Develop and execute a customer communications plan	<ul style="list-style-type: none"> <li>• Plans should include informing customers about the SCA-compliant authentication approaches, the SCA exemptions and out-of-scope of SCA transactions the Issuer intends,</li> <li>• Educational campaigns should be designed and executed as needed.</li> <li>• Issuers will need to report on customer communications to NCAs as required by the EBA opinion of 16 October 2019.</li> </ul>

## 6.2 Acquirer planning checklist



Acquirers should ensure they have a PSD2-SCA plan in place that covers at least the following critical decisions and actions:

**Table 41: Acquirer planning checklist**

1 Develop authentication and authorization strategies & policies		
1.1	Develop policies and systems for application of exemptions	<ul style="list-style-type: none"> <li>Develop risk management and exemption prioritization policies that will minimize the application of SCA challenges for low risk transactions while maintaining fraud rates within target reference fraud rates. For more guidance see Section 4.</li> <li>Exemption requests can be submitted through 3DS or direct to authorization <ul style="list-style-type: none"> <li>Work with merchants to optimize strategies that will optimize user experience while minimizing the risk of Issuers requesting Resubmission for authentication.</li> <li>Some Issuers want exemption requests to be sent in through 3DS. Identify those Issuers and refine your authorization strategies.</li> </ul> </li> </ul>
1.2	Develop risk policies to optimize application of the TRA exemption	<ul style="list-style-type: none"> <li>Define the reference fraud rate band(s) which you intend to comply with in order to apply the exemption.</li> <li>Analyze your fraud and risk management data to identify transaction profiles/risk scores for which the exemption can be applied while maintaining fraud rate below the target reference fraud rate threshold.</li> <li>Develop policies for selection of merchants for which you will offer to apply the TRA exemption taking account of: <ul style="list-style-type: none"> <li>Merchant fraud rates and the impact on liability and fraud count</li> <li>Merchant ability to apply transaction risk monitoring and assessment</li> </ul> </li> <li>Monitor the effectiveness of your TRA exemption policy in terms of measured. This includes fraud rate.</li> <li>Ensure you are meeting the fraud reporting and notification guidelines published by your NCA.</li> </ul>
2 Develop and execute a plan for ensuring all your merchants can support PSD2 SCA		
<ul style="list-style-type: none"> <li>The EBA Opinion published 21st June 2019 places a clear requirement on all Acquirers to develop and implement a plan with clear milestones to migrate all their merchants to solutions that support PSD2 SCA, to agree the plan with their Competent Authority and execute the plan in an expedited manner. A further opinion published by the EBA on 16 October 2019 has set the deadline by which the period of supervisory flexibility should end, and PSP migration plans should be complete as 31 December 2020. This opinion also sets out various requirements on PSPs to provide information and reporting to NCAs and provide information to merchants. In addition to development of these plans, Acquirers should take the following steps.</li> </ul>		

2.1	Ensure all your merchants are enabled for 3DS (including 3DS 1.0)	<ul style="list-style-type: none"> <li>Put in place a campaign to communicate the requirements of the PSD2 SCA regulation and the need to support 3DS in order to apply SCA</li> <li>Ensure merchants understand the requirements on them including having a 3DS Server provider, supporting the SDK and providing data elements</li> </ul>
2.2	Ensure your merchants understand the exemptions and the role they can play in optimizing the application of exemptions	<ul style="list-style-type: none"> <li>Work with merchants with sophisticated risk assessment capabilities to outsource the application of TRA and optimization the application of the exemption</li> <li>Ensure relevant merchants are aware of the potential of the trusted beneficiaries exemption and the need to educate their customers on enrollment</li> </ul>
2.3	Ensure merchants who submit out of scope transactions are able to flag them	<ul style="list-style-type: none"> <li>Merchants submitting MITs will need to support the MIT framework</li> </ul>
2.4	Ensure merchants are aware of the processing options and understand their obligations	<ul style="list-style-type: none"> <li>Proactively brief your merchant customers so that they understand the options available to them for applying exemptions and managing out of scope transactions via both 3DS and authorization flows</li> </ul>
<b>3 Ensure you and your merchants have the latest technology in place to optimize for PSD2</b>		
3.1	Plan to migrate to supporting EMV 3DS 2.2.0 as early as possible to ensure merchants can fully benefit from SCA exemptions	<ul style="list-style-type: none"> <li>All Acquirers should support EMV 3DS 2.2.0 as early as possible to ensure that exemptions can be fully supported.</li> <li>Acquirers should guide their merchants to migrate to EMV 3DS 2.2.0 in order to fully benefit from the support it provides in application of exemptions.</li> </ul>
3.2	Ensure you support the latest authorization field values	<ul style="list-style-type: none"> <li>Make sure you have coded to the new authorization fields</li> <li>If an Issuer responds with a response code 1A (SCA required), pass this to the gateway/merchant to have them trigger 3DS to retry the transaction</li> <li>Ensure gateways are aware of the new fields</li> <li>Look for abuse from merchants and monitor them / work with them</li> </ul>

## 6.3 Merchant planning checklist



All merchants with EEA Acquirers that take card payments will need to ensure that they can support 3-D Secure 2.0 by September 2019. This includes merchants who have not previously used 3-D Secure. Key actions merchants need to take are as follows:

**Table 42: Merchant planning checklist**

Action		Applies to	How to
1	Plan to adopt or migrate to EMV 3DS 2.2.0 as early as possible to ensure you can fully benefit from SCA exemptions	All merchants	<ul style="list-style-type: none"> <li>See steps below for more detailed guidance on key steps</li> </ul>
2	Implement a 3DS Server	All merchants	<ul style="list-style-type: none"> <li>If you already support 3-D Secure, consult your MPI vendor and/or payment service provider to agree an upgrade path to EMV 3DS</li> <li>If your current MPI vendor is unable to offer a 3DS Server capability you will need to select a new vendor with a certified 3DS Server product. Consult the Visa 3-D Secure Vendor list</li> <li>Ensure your vendor can provide access to all versions of 3DS including 3DS 1.0</li> <li>If you do not yet support 3-D Secure, you will need a 3DS Server vendor. If your e-commerce checkout functionality is hosted by a payment service provider on your behalf, you should consult your provider.</li> <li>Visa is able to offer a 3DS Server capability to merchants and Acquirers</li> </ul>
3	Ensure that mobile app-based checkouts support the EMV 3DS SDK	All merchants with mobile apps	<ul style="list-style-type: none"> <li>Consult the EMVCo 3-D Secure specification for more details on the SDK</li> <li>Identify a certified 3DS SDK vendor</li> </ul>
4	Ensure that you can provide all required data elements	All merchants	<ul style="list-style-type: none"> <li>Refer to Section 3.3.10 and Appendix A.1 for more details on the data elements</li> <li>Consult your 3DS server vendor or payment service provider to identify what action you need to take to ensure that data elements can be provided</li> </ul>
5	Ensure that you can support the Visa MIT framework	All merchants with subscription or other MIT payment business models	<ul style="list-style-type: none"> <li>Refer to Section 3.10 for more information on the MIT Framework and managing MITs</li> <li>Ensure procedures/systems are in place as soon as possible to store the transaction ID of a previous CIT or MIT to benefit from grandfathering of existing customer agreements already in place prior to 14 September 2019</li> </ul>

			<ul style="list-style-type: none"> <li>Consult your Acquirer if required for additional detailed guidance</li> </ul>
6	Work with your Acquirer to develop exemption strategies that respond to your business needs	Merchants who take a sophisticated approach to risk management and checkout user experience optimization	<ul style="list-style-type: none"> <li>Consider whether you would benefit from your Acquirer applying the TRA exemption and/or the trusted beneficiaries exemption.</li> <li>Agree with your Acquirer that they are prepared to apply the TRA exemption on your behalf and whether you will undertake</li> <li>Refer to Sections 4.3.1 and 4.5 for more guidance on considerations to take into account</li> </ul>
7	Plan to make use of the trusted beneficiaries exemption	Merchants with regular returning customers who are able to demonstrate a low fraud rate.	<ul style="list-style-type: none"> <li>Consider whether to participate in the Visa Trusted Listing program (for more details refer to Section 3.6)</li> <li>Consider how to explain the benefits of trusted beneficiaries listing to your customers and encourage those whose Issuers support it to enroll you</li> </ul>

# 7. Bibliography

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

**Table 43: 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.
Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure	Version 1.1, 21 August 2019	The Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure contains operational guidance for Merchants and Acquirers on the Visa implementation of 3-D Secure including:
Visa Secure Issuer Implementation Guide for EMV 3-D Secure	Version 1.1, 21 August 2019	The Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure contains operational guidance for Merchants and Acquirers on the Visa implementation of 3-D Secure including
Visa Secure Program Guide – Visa Supplemental Requirements	Version 1.1 8 <sup>th</sup> August 2019	This document is for Visa Secure and its use to support authentication of payment transactions
European EMV 3DS 2.2.0 Implementation Guide	Version 1.0 30 October 2019	Provides a summary of the features, benefits and implementation considerations for EMV 3DS 2.2.0
Visa Secure Cardholder Authentication Verification Value (CAVV) Guide	Version 3.0 April 2019	Provides detailed information on CAVV creation and verification and use in authorization for both 3DS 1.0 and EMV 3DS.
PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements	Version 1.0 October 2019	Guide summarizing Visa Rules relevant to the application of PSD2 SCA.



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	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.
VisaNet Business Enhancements Global Technical Letter and Implementation Guide.	October 2019 Version 3.0 (Major Release) and January 2020 Version 2.0 (Minor Release) – effective 5 September 2019	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.
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.
Visa Trusted Listing Program Implementation Guide	Version 1.0 9 <sup>th</sup> April 2019	Describes the Visa Trusted Listing Program and provides practical guidance to Issuers, Acquirers, technology providers, and merchants who participate in the Visa Trusted Listing Program on implementation and usage of the solution.
Visa Transaction Advisor Implementation Guide	Version 1.0 August 2019	Describes the Visa Transaction Advisor and provides practical guidance to Issuers, Acquirers, technology providers, and merchants who use the Visa Transaction API or its results on implementation and usage of the solution.
Visa Transaction Advisor API Specification	9th May 2019	Details the data elements required for the VTA API request and expected API response fields.
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.

# Glossary

**Table 44: Glossary of terms**

Term	Description
1-9	
3-D Secure (3DS) 2.0	<p>The Three Domain Secure (3-D Secure™ or 3DS) Protocol has been developed to improve transaction performance online and to accelerate the growth of e-commerce. The objective is to benefit all participants by providing Issuers with the ability to authenticate customers during an online purchase, thus reducing the likelihood of fraudulent usage of payment cards and improving transaction performance.</p> <p>Visa owns 3DS 1.0.2 and licenses it to other payment providers. EMVCo owns EMV 3DS.</p> <p>Visa's offering of 3DS is called Visa Secure.</p>
3-D Secure Server (3DS Server)	A server or system that the merchant (or third party on the merchant's behalf) uses to support Visa's EMV 3DS Program authentication processing.
A	
Access Control Server (ACS)	A server hardware/software component that supports Visa's EMV 3DS Program and other functions. The ACS is operated by the Issuer or the Issuer's processor. In response to Visa Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the customer, and provides digitally-signed authentication response messages (containing the authentication results and other Visa's EMV 3DS Program data) to the merchant.
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 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 a Visa account to another account.

Term	Description
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	
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.
C	
Cardholder Authentication Verification Value (CAVV)	A unique value transmitted in response to an Authentication Request.
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>

Term	Description
<b>D</b>	
Delegated Authentication	Issuers can delegate authentication to an Acquirer and in turn their qualified Delegates. Visa Delegated Authentication provides the framework and conditions for Issuers within the Visa ecosystem to delegate authentication to Delegates that meet stringent qualification criteria.
Device Binding	The process of verifying that the Issuer's cardholder has possession of the device on which the token is being used or provisioned to by performing Issuer authentication when the binding is established. Device binding also includes account binding by default. Device binding can occur during token provisioning or as a standalone action. Device binding links a token to a specific Token Requestor's device id and enables the linked device to satisfy the possession factor for SCA where the Token Requestor can reliably and unambiguously identify the device.
Directory Server (DS)	An EMVCo 3DS server component operated in the Interoperability Domain; it performs a number of functions that include: authenticating the 3DS Server, routing messages between the 3DS Server and the ACS, and validating the 3DS Server, the 3DS SDK, and the 3DS Requestor.
Dispute	A Transaction that an Issuer returns to an Acquirer.
Dynamic Linking	The process of associating the transaction to a payment amount and payee at the time of transaction processing
<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>• Secured corporate payment exemption</li> <li>• Transaction Risk Analysis</li> </ul>

Term	Description
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 1.
L	
Liability	Any and all damages (including lost profits or savings, indirect, consequential, special, exemplary, punitive, or incidental), penalties, fines, expenses and costs (including reasonable fees and expenses of legal and other advisers, court costs and other dispute resolution costs), or other losses.
M	
Merchant Initiated Transaction (MIT)	A transaction, or series of transactions, of a fixed or variable amount and fixed or variable interval governed by an agreement between the cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the cardholder. Applies to all payment instruments including cards.
O	
Original Credit Transaction (OCT)	A Transaction initiated by a Member either directly, or on behalf of its Merchants, that results in a credit to a Visa Account Number for a purpose other than refunding a Visa purchase.
Out-Of-Band (OOB) Authentication	A Challenge activity that is completed outside of, but in parallel to, the 3-D Secure flow. The final Challenge Request is not used to carry the data to be checked by the ACS but signals only that the authentication has been completed.
P	
Primary Account Number (PAN)	The Primary Account Number (PAN) is the number embossed and/or encoded on payment cards and tokens that identifies the card Issuer and the funding account and is used for transaction routing. PAN normally has 16 digits but may be up to 19 digits.

Term	Description
Payment Facilitator	A vendor or service provider that is not a regulated Acquirer but is providing services on behalf of a merchant enabling that merchant to authenticate and/or accept electronic payments.
PSD2	The Second European Payment Services Directive whose requirements include that Strong Customer Authentication is applied all electronic payments where both Issuer and Acquirer are within the European Economic Area (EEA). This requirement is effective as of 14 September 2019 <sup>97</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).
R	
Reference Fraud Rate (RFR)	The benchmark maximum fraud rate, defined by the PSD2 SCA RTS, that a PSP's calculated fraud rate must be equivalent to or below in order for that PSP to qualify to apply the TRA exemption to a transaction of a specified value. The PSD2 SCA RTS defines three reference fraud rates for three transaction value bands, each defined by an ETV.
Regulatory Technical Standards (RTS)	<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>
S	

<sup>97</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
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.
Tokenization	Tokenization is the process of replacing the traditional payment card account number with a unique digital token in online and mobile transactions
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



Term	Description
	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.
Visa Secure	Visa's consumer brand name for EMV 3DS
Visa Token Service	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.
Visa TRA Program	Visa has established a set of conditions for the adoption and subsequent use of VTA to inform the application of the TRA exemption. This is referred to as the "Visa TRA program".
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 EMV 3DS Data Elements

Merchants must provide the data elements in EMV 3DS authentication message as follows: 1) required always and 2) required if available. Merchants are also required to use the 3DS Method if the Method URL is provided by the Issuer. Providing EMV 3DS data is subject to regional and country regulations.

The merchant data has been categorized into seven groups.

**Table 45: Transactional and checkout page information**

Data Element	Required Always	Required if Available	Browser only (B) or SDK only (S)
3DS Method Completion Indicator	●		
3DS Requestor Authentication Indicator		●	
3DS Challenge Indicator	●		
3DS Requestor ID	●		
3DS Requestor Name	●		
3DS Requestor URL	●		
3DS Server Operator ID	●		
3DS Server Reference Number	●		
3DS Server Transaction ID	●		
3DS Server URL	●		
3RI Indicator		●	
Account Type		●	
Acquirer BIN	●		
Acquirer Merchant ID	●		
Address Match Indicator		●	
Broadcast Information		●	
Browser Accept Headers	●		
Browser IP Address		●	B

Browser Java Enabled	●		<b>B</b>
Browser Language	●		<b>B</b>
Browser Screen Color Depth	●		<b>B</b>
Browser Screen Height	●		<b>B</b>
Browser Screen Width	●		<b>B</b>
Browser Time Zone	●		<b>B</b>
Browser User-Agent	●		<b>B</b>
Card/Token Expiry Date	●		
Cardholder Account Identifier		●	
Cardholder Account Number	●		
Cardholder Billing Address City	●		
Cardholder Billing Address Country	●		
Cardholder Billing Address Line 1	●		
Cardholder Billing Address Line 2	●		
Cardholder Billing Address Line 3	●		
Cardholder Billing Address Postal Code	●		
Cardholder Billing Address State	●		
Cardholder Email Address	●		
Cardholder Home Phone Number		●	
Cardholder Mobile Phone Number		●	
Cardholder Name	●		
Cardholder Shipping Address City		●	
Cardholder Address Country		●	
Cardholder Shipping Address Line 1		●	
Cardholder Shipping Address Line 2		●	
Cardholder Shipping Address Postal Code		●	
Cardholder Shipping Address State		●	
Cardholder Work Phone Number		●	
Device Channel	●		

Device Rendering Options Supported	●		<b>S</b>
EMV Payment Token Indicator		●	
Installment Payment Data		●	
Merchant Category Code	●		
Merchant Country Code	●		
Merchant Name	●		
Message Category	●		
Message Extension		●	
Message Type	●		
Message Version Number	●		
Notification URL	●		
Purchase Amount	●		<b>B</b>
Purchase Currency	●		
Purchase Currency Exponent	●		
Purchase Date & Time	●		
Recurring Expiry		●	
Recurring Frequency		●	
SDK App ID	●		<b>S</b>
SDK Encrypted Data	●		<b>S</b>
SDK Ephemeral Public Key (Qc)	●		<b>S</b>
SDK Maximum Timeout	●		<b>S</b>
SDK Reference Number	●		<b>S</b>
SDK Transaction ID	●		<b>S</b>
Transaction Type	●		

For more information on 3DS Server Identifiers listed in the above table see *Visa Secure – Merchant/Acquirer Implementation Guide for EMV 3-D Secure*.

**Table 46: 3DS Requestor authentication information**

Data Element	Required Always	Required if Available	Browser only (B) or SDK only (S)
3DS Requestor Authentication Method	●		
3DS Requestor Authentication Timestamp		●	
3DS Requestor Authentication Data		●	

**Table 47: 3DS Requestor prior transaction authentication information**

Data Element (3DS Requestor Prior Transaction:)	Required Always	Required if Available	Browser only (B) or SDK only (S)
Reference		●	
Authentication Method		●	
Authentication Timestamp		●	
Authentication Data		●	

**Table 48: Merchant risk indicator**

Data Element	Required Always	Required if Available	Browser only (B) or SDK only (S)
Shipping Indicator		●	
Delivery Timeframe		●	
Delivery Email Address		●	
Reorder Items Indicator		●	
Pre-Order Purchase Indicator		●	
Pre-Order Date		●	
Gift Card Amount		●	
Gift Card Currency		●	
Gift Card Count		●	

**Table 49: Cardholder account information**

Data Element	Required Always	Required if Available	Browser only (B) or SDK only (S)
Cardholder Account Age Indicator		●	
Cardholder Account Date		●	
Cardholder Account Change Indicator		●	
Cardholder Account Change		●	
Cardholder Account Password Change Indicator		●	
Cardholder Account Password Change		●	
Shipping Address Usage Indicator		●	
Number of Transactions Day		●	
Number of Transactions Year		●	
Number of Provisioning Attempts Day		●	
Cardholder Account Purchase Count		●	
Suspicious Account Activity		●	
Shipping Name Indicator		●	
Payment Account Age Indicator		●	
Payment Account Age		●	

**Device information (required for mobile app)**

Device information must be provided if a mobile app is being used by the cardholder.

**3DS Method**

The merchant checkout page must load the ACS 3DS Method URL, if the 3DS Method URL is present, which allows the ACS to obtain additional browser information for risk-based decision making.

## A.2 Appendix 2 Authentication Message Fields

**Table 50: Visa Authentication messages, message values and how they are used.**

Message Type	Message Response Data			
Message	Transaction Status	Transaction Status Description	ECI	CAVV
<b>Authentication Request /Response (AReq/ARes)</b> The 3DS Server <sup>98</sup> sends the AReq through the Visa Directory Server to the Issuer ACS or Attempts ACS Upon receipt, the Issuer ACS or Attempts ACS performs risk-based authentication and provides the results of authentication to the 3DS Server in the Ares	Y	Authentication Successful	05	CAVV Present
	A	Attempts Processing Performed	06	
	N	Authentication Failed; Not Authenticated; Transaction Denied	07	No CAVV
	U	Authentication Could Not Be Performed; Technical or Other Problem		
	C	Challenge Required to authenticate the cardholder		
	R	Authentication Rejected		
<b>Challenge Request/Response (CReq/CRes)</b> The 3DS Server (or 3DS SDK) sends the CReq to the Issuer ACS Upon receipt, the Issuer ACS challenges the cardholder through an authentication method such as OTP	Y	Authentication Successful	Results of the challenge are sent in the Results Request (RReq) message by the ACS to the 3DS Server.	
	N	Not Authenticated; Transaction Denied		

<sup>98</sup> 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.

and responds to the 3DS Server or 3DS SDK with the Cres			
<b>Results</b> <b>Request/Response (RReq/RRes)</b>  The Issuer ACS sends the RReq to the 3DS Server to provide the results of the challenge authentication  The 3DS Server acknowledges the RReq by responding with the RRes			
	Same set of values as AReq/Ares <ul style="list-style-type: none"> <li>• A successful challenge is an ECI 05 with a CAVV</li> <li>• An unsuccessful challenge is an ECI 07 with no CAVV</li> </ul>		

For more details on how these messages are used in the Frictionless and Challenges authentication flows, please refer to *Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure*.

Flags may also be set in AReq message to indicate the application of exemptions. These are summarized in table 36 below.



**Table 51: Flags Set in AReq Message to indicate the application of exemptions**

3DS Field	Purpose	Value
<b>Challenge Indicator</b> Field Name: threeDSRequestorChallengeInd	Indicates whether a challenge is requested for this transaction. For example: <ul style="list-style-type: none"> <li>For 01-PA, a 3DS Requestor may have concerns about the transaction, and request a challenge.</li> <li>For 02-NPA, a challenge may be necessary when adding</li> </ul>	01 = No preference 02 = No challenge requested 03 = Challenge requested (3DS Requestor preference) 04 = Challenge requested (Mandate) 05 = No challenge requested (transactional risk analysis is already performed) 06 = No challenge requested (Data share only) 07 = No challenge requested (strong customer authentication is already performed) 08 = No challenge requested (utilize whitelist exemption if no challenge required) 09 = Challenge requested (whitelist prompt requested if challenge required)
<b>3DS Requestor Authentication Indicator</b> Field Name: threeDSRequestorAuthenticationInd	Indicates the type of Authentication request. This data element provides additional information to the ACS to determine the best approach for handing an authentication request.	01 = Payment transaction 02 = Recurring transaction 03 = Installment transaction 04 = Add card 05 = Maintain card 06 = Cardholder verification as part of EMV token ID&V 07–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) 80–99 = Reserved for DS use

## A.3 Appendix 3 Considerations for Implementing OOB Biometrics on EMV 3DS 2.1.0 and 2.2.0

### A.3.1 Introduction

OOB authentication allows users to authenticate themselves using a separate app, for example their mobile banking application, while making a purchase at a merchant website or app.

The generic OOB authentication process flow is as follows:

1. The customer initiates the transaction via the secure checkout in the merchant's desktop or mobile website or app
2. The customer is prompted to open the OOB authentication app
3. Authentication is completed via the OOB authentication app
4. The customer is prompted to switch back to the browser or merchant app or may be automatically returned to the browser or merchant app (EMV 3DS 2.2.0 desktop browser and app only) to complete the transaction.

The below sections highlight important considerations and recommendations for Issuers and ACS providers implementing OOB authentication.

Table 52 below summarizes OOB authentication UX functionality supported by EMV 3DS 2.1.0 and EMV 3DS 2.2.0.

**Table 52: OOB authentication UX functionality by EMV 3DS version**

	Supported by EMV 3DS 2.1.0	Supported by EMV 3DS 2.2.0
<b>Browser experience</b>		
• Navigating to the OOB Authentication App	Yes	Yes
• Navigating from the OOB Authentication App back to the mobile browser after authentication	No	No
• Automatically proceeding with the purchase flow after OOB authentication	Yes	Yes
<b>App experience</b>		
• Navigating to the OOB Authentication App	Yes	Yes
• Navigating from the OOB Authentication App back to the mobile app after authentication	No	Yes
• Automatically proceeding with the purchase flow after OOB authentication	No	Yes

Visa strongly recommends that Issuers and ACS providers wishing to implement OOB authentication only do so if they support EMV 3DS 2.2.0. The OOB user experience delivered by EMV 3DS 2.1.0 is confusing to customers and is likely to result in a high level of authentication failures due to customer mis-operation. The reasons for this are that:

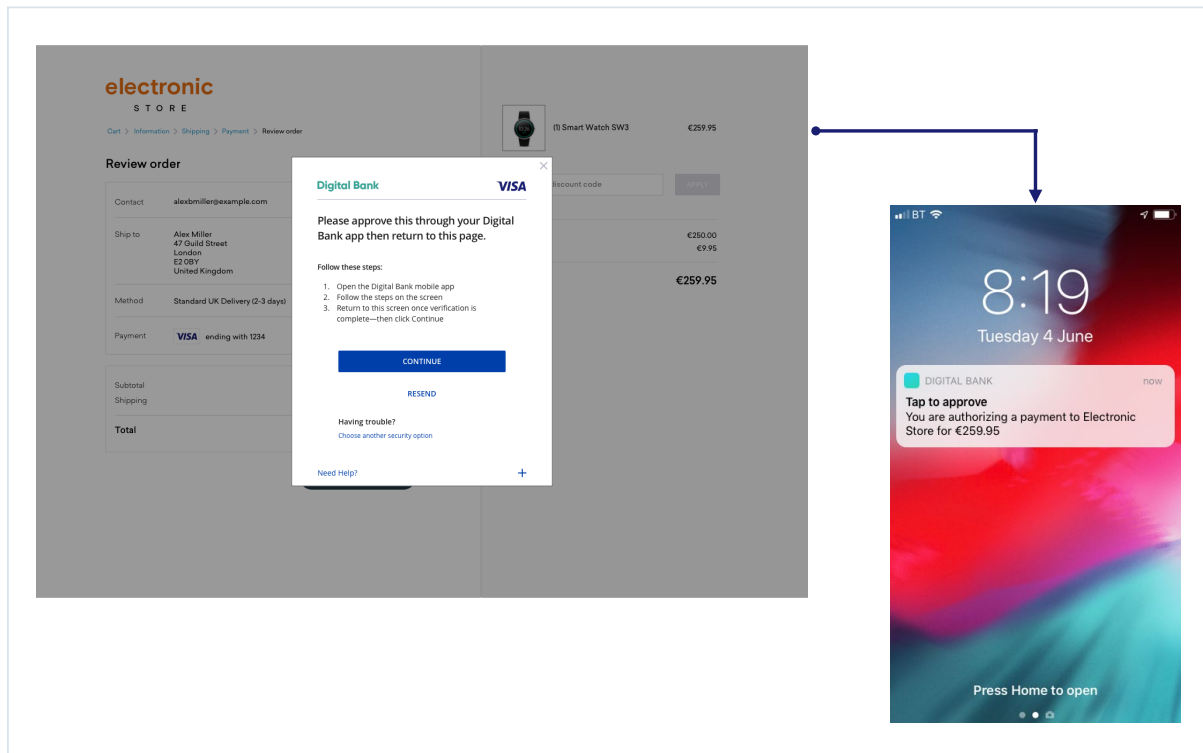
- The secure checkout prompt to open the OOB app includes a prominent “continue” button that customers should only select once they have successfully completed the authentication through the separate online banking app. The presentation of this button is such that customers are very likely to select it before completing authentication, resulting in repeated error messages,
- EMV 3DS 2.1.0 does not support automatic return to the merchant’s secure mobile web or app checkout, again potentially resulting in transaction abandonment.

### A.3.2 Recommendations for optimizing consumer experience applicable to desktop and mobile browser and app flows

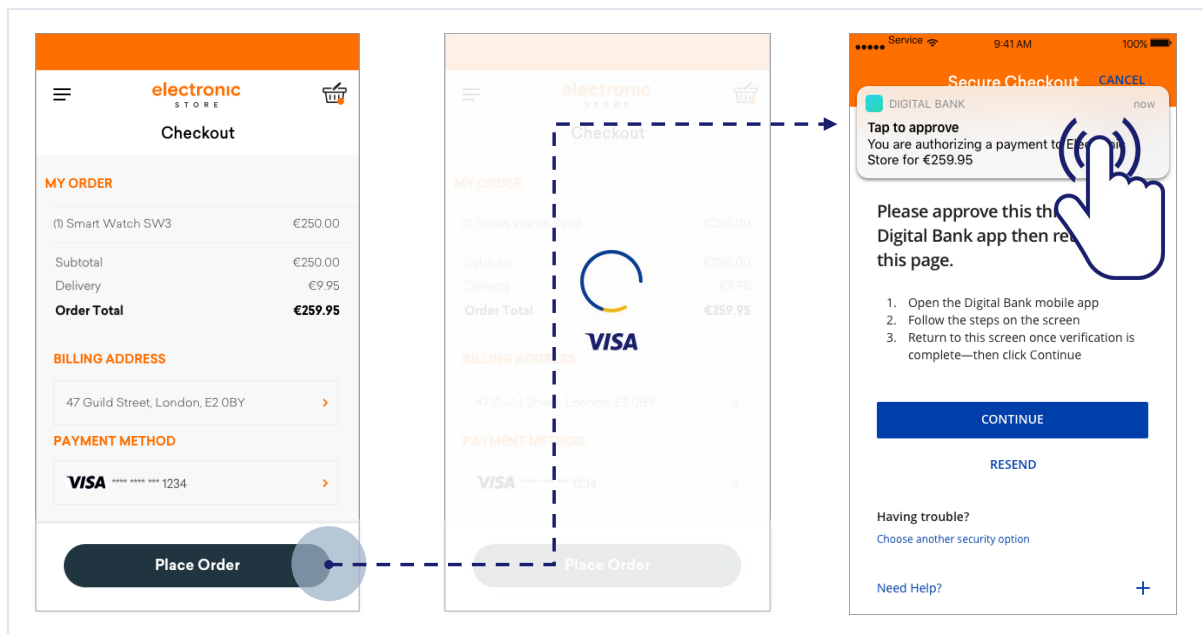
The following suggestions are applicable for implementations across desktop browser, mobile browser and native app:

- A push notification should be sent to the customer’s phone which, when clicked, includes a link that automatically opens the consumer’s OOB app to perform authentication (see Figures 27 and 28 below). **(Issuer)**
- If the customer doesn’t have the OOB app on their phone, the Issuer/ACS should provide an alternative authentication solution. **(Issuer)**
- Instructions should be shown for the customer to open their banking application to perform authentication, particularly in the circumstance that push notifications are not available or enabled. **(Issuer)**
- If the customer clicks “Continue” before performing the authentication using the OOB app, the ACS will present the challenge screen and highlight to the cardholder to authenticate with the OOB app before clicking “Continue” (see Figure 27 below). Warning: The prominence of the “Continue” button in the EMV 3DS 2.1.0 UX makes it probable that customers will select it in error leading to authentication failures.

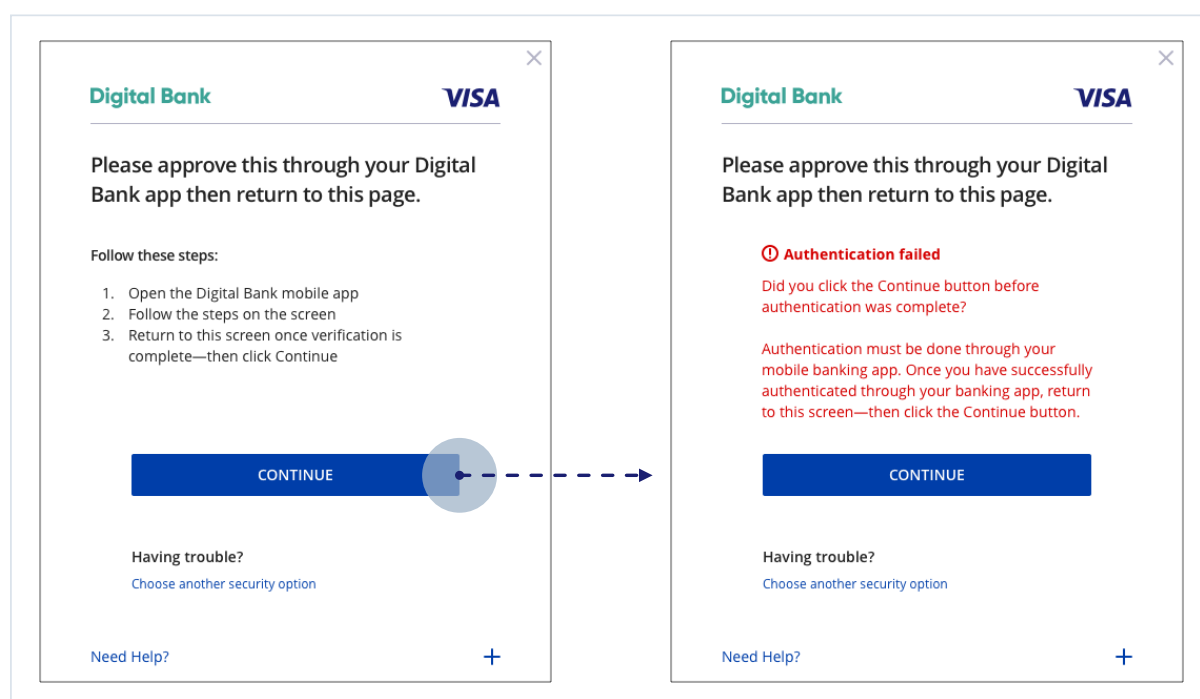
**Figure 27: Sending a push notification to prompt customers to open their mobile banking app – desktop browser**



**Figure 28: Sending a push notification to prompt customers to open their mobile banking app - mobile browser or app**



**Figure 29 Clicking 'Continue' before authentication is complete will result in an error**



### A.3.3 Additional recommendations relevant to desktop browser purchases

The following additional suggestion is applicable for desktop browser implementations:

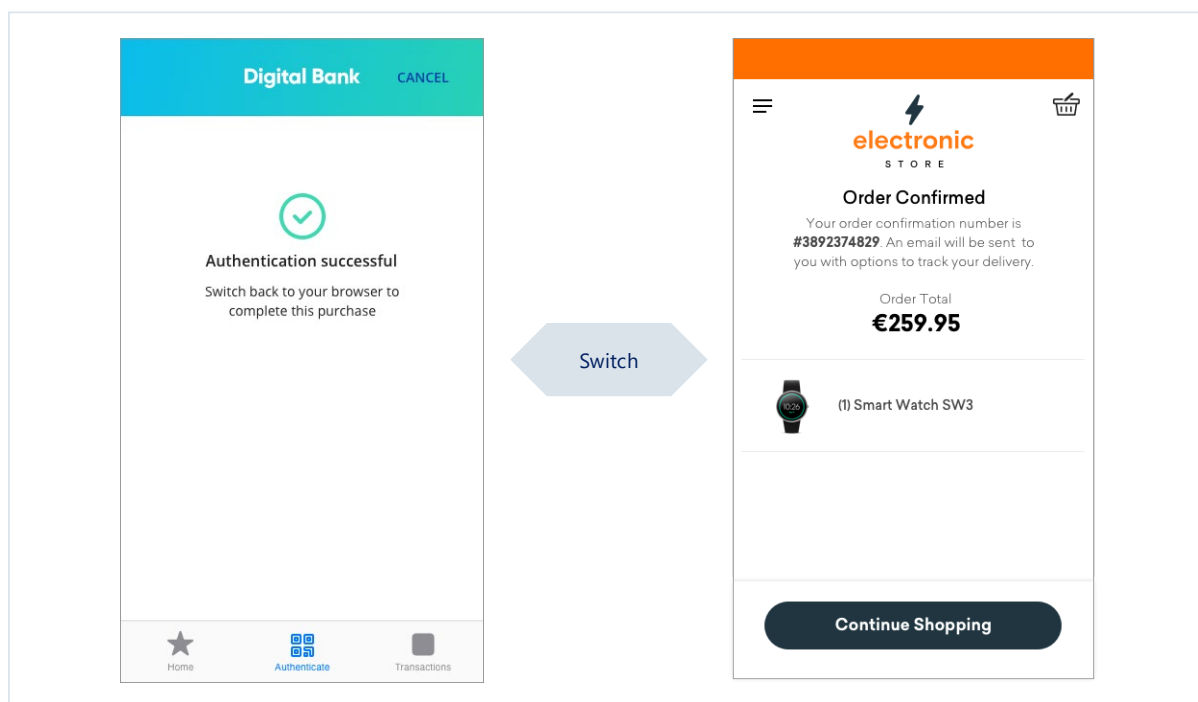
- The desktop browser merchant webpage should automatically refresh and take the consumer to merchant checkout completion page. This can be done by, for example, by the ACS implementation constantly checking the Issuer server for completion of authentication and then automatically proceeding with the rest of the purchase flow, refreshing the webpage to show the checkout completion. **(ACS)**

### A.3.4 Additional recommendations relevant to mobile browser purchases

The following additional suggestions are applicable for mobile browser implementations:

- The ACS should allow the OOB app to launch from a browser page on the same mobile device, i.e., by providing a button/link that launches the OOB app for the consumer to perform authentication. **(ACS)**
- The 3-D Secure 2.1.0 and 2.2.0 specifications do not provide a way to automatically return to the merchant's website on a mobile browser. The customer must manually open the mobile browser after OOB authentication to complete merchant checkout. The OOB app should present the customer with clear instructions to return to the merchant site after successful authentication (see figure 30 below). **(Issuer)**

**Figure 30: After successful authentication, customers must manually open the mobile browser to see the order confirmation screen**



### A.3.5 Additional recommendations relevant to mobile app purchases

This section is specific to native apps. For hybrid apps and web apps, please refer to Section A 3.2.

Best Practice for Optimizing Consumer Experience:

- Issuers are advised not to offer OOB authentication for mobile app flows using EMV 3DS 2.1.0 as specifications do not provide a way to automatically return to the merchant's website on mobile browser.
- The 3-D Secure 2.2 specifications provide a method for the OOB authentication app to automatically return to the merchant app. This can be accomplished through the threeDSRequestorAppURL field.
- The EMV 3DS 2.2.0 SDK detects that the merchant app is taken to the background in terms of activity status when the OOB app is opened. When the customer is re-directed back to the merchant app, the EMV 3DS 2.2.0 SDK can detect the return and automatically proceed to the completion screen.

**Figure 31: Mobile app user experience flow showing push notification prompt to open mobile banking app and automatic return on successful authentication.**



## A.4 Appendix 4 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 53: Key data fields for performing CIT transactions with stored credentials**

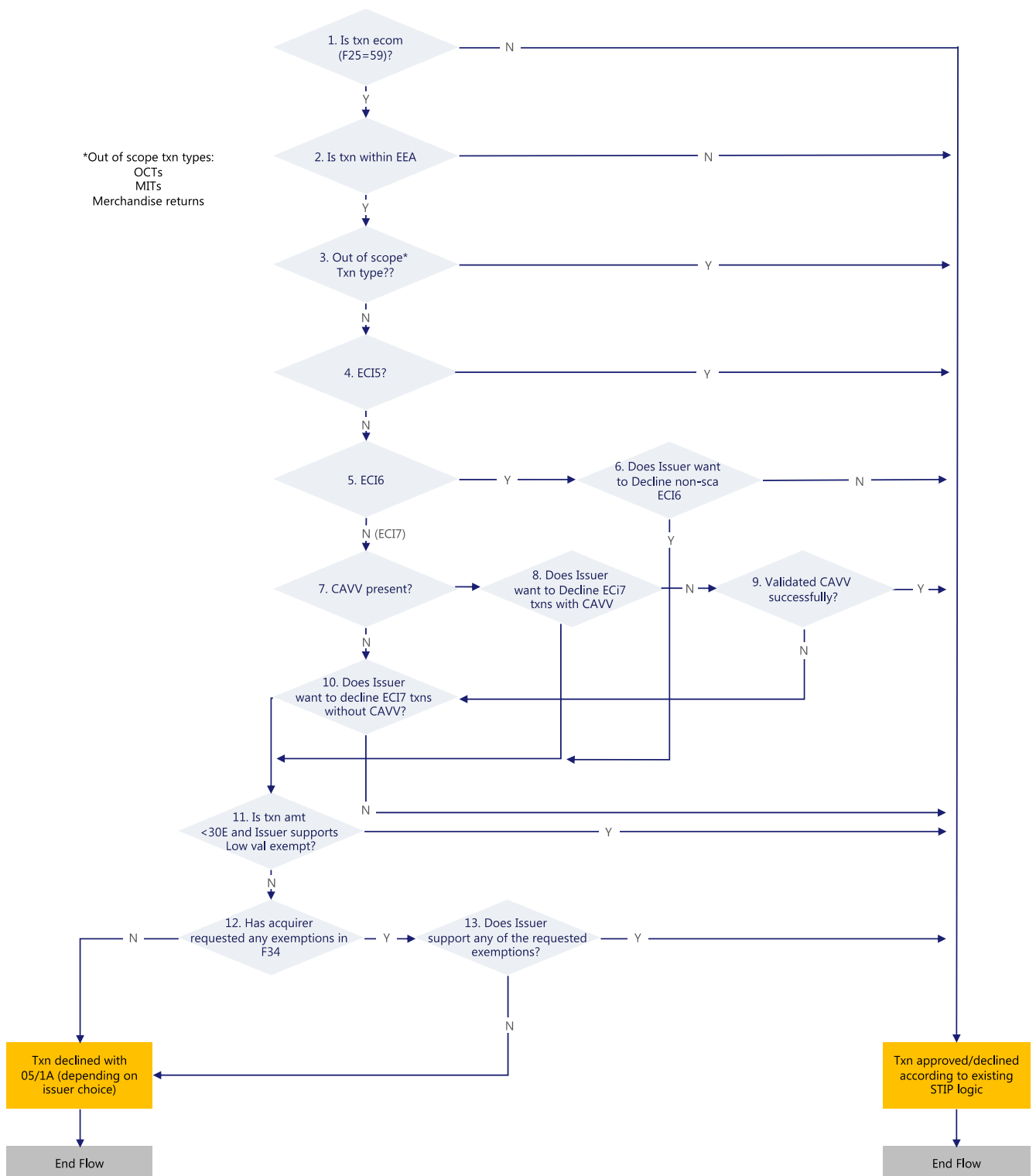
Transaction Type	Description	POS Entry Mode (F22)	POS environment (F126.13)
CIT	Customer Initiated (CIT) – putting credential on file for first time (e.g. for future use; may be done during a transaction or at account set up via an account verification transaction)	01	C
CIT	Subsequent CIT performed with 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 3.10.



## A.5 Appendix 5 STIP SCA Flowchart

Figure 32: STIP SCA flowchart



## A.6 Appendix 6 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 standing 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

Digital payment made via an app to purchase goods or order services at the customer's request, such as ordering a ride via an app or buying train tickets, are not MITs but are considered CITs as the cardholder actively participates in the transactions.

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.6.1 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.6.2 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	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).
Relevant Merchant Segments	<p>Incremental transactions are limited to certain merchant categories. Examples include car rental, lodging, transit, amusement parks, restaurants, and bars.</p> <p>For complete list of all eligible MCCs, refer to the Visa Rules (ID#: 0025596).</p>
Examples	A lodging merchant performs an incremental authorization while adding room service expenses to cardholder's folio, revising previous estimate of cardholder's total charges

### A.6.3 Resubmission Transaction—Reason Code 3901 in Field 63.3—Message Reason Code

Description	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.
Maximum Timeframe between Original Transaction and MIT	Resubmission must be submitted within 14 days from the original transaction. This timeframe limit only applies to token-based resubmissions.
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.6.4 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.6.5 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 eCommerce 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, eCommerce 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 eCommerce retail, lodging, car rental, and cruise lines.

Examples	Any merchant category can submit Reauthorization. This type of transaction is most prevalent in eCommerce retail, lodging, car rental, and cruise lines.
----------	---

#### A.6.6 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.6.7 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.6.8 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.6.9 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.6.10      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.7 Appendix 7 EEA Countries in scope of PSD2 SCA

The countries below represent those participating in the European Economic Area and therefore subject to PSD 2 regulation

**Table 54 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
GIBRALTAR GI 292	SLOVAKIA SK 703
GREECE GR 300	SLOVENIA SI 705
HUNGARY HU 348	SPAIN ES 724
ICELAND IS 352	SWEDEN SE 752
IRELAND IE 372	UNITED_KINGDOM GB 826

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 and Visa representative to determine if SCA applies and if so how to comply and optimize.