



# PSD2 SCA Secure Corporate Payment Exemption Guide

June 2021

Version 1.2  
24 June 2021

**VISA**

# Contents

---

<b>Important Information .....</b>	<b>4</b>
<b>1. Introduction, purpose &amp; scope of this guide.....</b>	<b>5</b>
<b>2. The SCP ecosystem &amp; use of terminology .....</b>	<b>6</b>
<b>3. Interpreting the regulation regarding the Secure Corporate Payment exemption...7</b>	
3.1 The key provisions of the regulation .....	7
3.2 Interpreting the exemption .....	7
3.3 Examples of secure dedicated payment processes or protocols.....	8
<b>4. Applying the SCP exemption.....</b>	<b>9</b>
4.1 Introduction to the use of the SCP exemption and the SCP exemption indicator .....	9
4.2 Applying the SCP exemption to transactions using different types of Commercial Card product .....	10
4.3 Routing transactions with the SCP exemption indicator .....	11
4.4 The SCP exemption via EMV 3DS .....	12
4.5 The SCP exemption indicator in authorization .....	13
4.6 Recognition of the indicator and application of the exemption by the Issuer.....	13
4.7 Frameworks of Controls & Visa requirements.....	13
<b>5. Additional Impacts for Issuers.....</b>	<b>16</b>
5.1 Demonstrating qualification to NCAs .....	16
5.2 Supporting the SCP exemption indicator .....	16
5.3 Meeting the requirements of the framework of controls.....	17
5.4 Encouraging the use of qualifying card products in secure corporate environments	17
5.5 Considering the use of other exemptions for non-qualifying Commercial Card transactions .....	17
5.6 FCA requirements on Issuers (UK Only).....	17
5.7 The need to communicate with and support corporate customers.....	18
<b>6. Additional impacts for Acquirers .....</b>	<b>18</b>
6.1 Supporting merchants with the use of the SCP exemption indicator.....	18
6.2 Meeting Visa’s framework of controls requirements for use of the SCP exemption indicator .....	19
<b>7. Additional impacts for merchants &amp; intermediaries processing transactions on behalf of merchants .....</b>	<b>19</b>
7.1 Merchant use of the SCP exemption indicator .....	19

7.2	Impacts on intermediaries processing bookings or orders on behalf of merchants	21
<b>8.</b>	<b>Example Use cases</b>	<b>22</b>
8.1	Corporate travel booking made via a TMC/CBT	22
8.2	Travel booking B2B payment between an online travel agent & supplier using a virtual card	26
<b>9.</b>	<b>Bibliography</b>	<b>28</b>
<b>10.</b>	<b>Glossary</b>	<b>30</b>
<b>A</b>	<b>Appendices</b>	<b>35</b>
A.1	Framework of Controls & Visa requirements	35
A.2	Appendix 2 –SCP exemption fraud liability table	37

# Important Information

---

© 2021 Visa. All Rights Reserved.

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

Disclaimer: Case studies, comparisons, statistics, research and recommendations are provided “AS IS” and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice.

As a new regulatory framework in an evolving ecosystem, the requirements for SCA still need to be refined for some use cases. This paper represents Visa’s evolving thinking, but it should not be taken as a definitive position or considered as legal advice, and it is subject to change in light of competent authorities’ guidance and clarifications. Visa reserves the right to revise this guide pending further regulatory developments.

This guide is also not intended to ensure or guarantee compliance with regulatory requirements. Payment Service Providers are encouraged to seek the advice of a competent professional where such advice is required.

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

Note on references to EMV 3DS: When in this document we refer to EMV 3DS, this is a generic reference to the second generation of 3-D Secure and does not reference a specific version of the EMVCo specification. Version 2.1 of the specification is referred to as EMV 3DS 2.1 and version 2.2 is referred to as EMV 3DS 2.2.

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

# 1. Introduction, purpose & scope of this guide

---

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

The requirement to apply SCA came into force on 14 September 2019. In relation to e-commerce, the European Banking Authority (EBA) has recognised the need for a delay in enforcement to allow time for all parties in the payments ecosystem to fully implement SCA, setting a deadline of 31 December 2020 by which time the period of supervisory flexibility was to have ended. The migration plans of PSPs, including the implementation and testing by merchants should also have been completed by 31 December 2020. While the majority of National Competent Authorities (NCAs) have now aligned with the EBA's guidance, PSPs should check with NCAs for enforcement timescales in their respective markets since in some jurisdictions local regulators may be exercising some short term flexibility in enforcement during at least the initial part of 2021. As regards the UK, the Financial Conduct Authority (FCA) will start to enforce the regulation which transposes PSD2 into UK law from 14 September 2021 in relation to e-commerce (subject to compliance with phased implementation plans).

The PSD2 SCA Regulatory Technical Standards (RTS) includes the secure corporate processes and protocols exemption, referred to in this guide as the Secure Corporate Payment (SCP) exemption. Under this exemption, SCA may not need to be applied to some corporate transactions so long as certain conditions are met. There are a number of considerations to take into account in terms of interpretation and governance of the regulation around this exemption and its practical application.

In many cases it will not be possible to authenticate transactions originating in a secure corporate environment and requesting SCA may result in valid transactions being declined. Issuers of virtual cards, Central Travel Accounts (CTAs) and lodged accounts should specifically note that not supporting the exemption will result in a high rate of declines for transactions using these products, as it is not possible to authenticate transactions that do not qualify for any other exemption, and this will challenge the viability of continuing to issue these products.

Issuers of Commercial Cards are therefore strongly encouraged to support the SCP exemption and merchants who process transactions originating from secure corporate purchasing systems or travel management systems should discuss with their Acquirer to determine whether any of their transactions should/could be flagged to their Acquirer with the SCP exemption indicator<sup>1</sup>.

This guide aims to provide a clear single point of reference summarising Visa's view on the regulatory interpretation of the SCP exemption, requirements governing application of the exemption and providing guidance on the practical steps that Payment Service Providers (PSPs), merchants and other stakeholders need to take to make use of the exemption.

---

<sup>1</sup> This enables a transaction to be processed without authentication, so long as certain conditions are met, including that the Issuer supports the exemption, and the payer qualifies as a "legal person". See section 4.1 for more information.

This guide is not intended to provide legal advice nor to ensure or guarantee compliance with regulatory requirements. Payment Service Providers and merchants are encouraged to seek the advice of a competent professional where such advice is required.

## 2. The SCP ecosystem & use of terminology

---

Corporate purchases and travel bookings and associated transaction processes commonly involve multiple parties. The following terminology has been adopted in this guide to describe these parties:

- **Corporate:** The corporate customer that is the ultimate payer for the product or service being purchased and to whom and/or whose staff Commercial Cards have been issued.
- **Merchant:** The ultimate recipient of the funds at settlement of a transaction (i.e. the entity whose name is in the "Card Acceptor Name/Location" field in the Visa transaction).
- **Booking/Purchasing Portal:** An entity that provides a secure travel booking or B2B purchasing environment and initiates reservations/orders on behalf of the corporate. Examples include corporate Travel Management Companies (TMCs), Corporate Booking Tools (CBTs) and purchasing systems.
- **Aggregator/Reservation System:** An entity that sits between the corporate, or the booking/purchasing portal and the merchant and performs one or more of the following functions:
  - Provides content into a booking or purchasing system;
  - Passes booking or purchasing and transaction data between the entity making the booking or purchase and the merchant;
  - In some cases, undertakes part of the transaction's authorization, clearing and settlement process on behalf of the merchant while not being the merchant's Acquirer

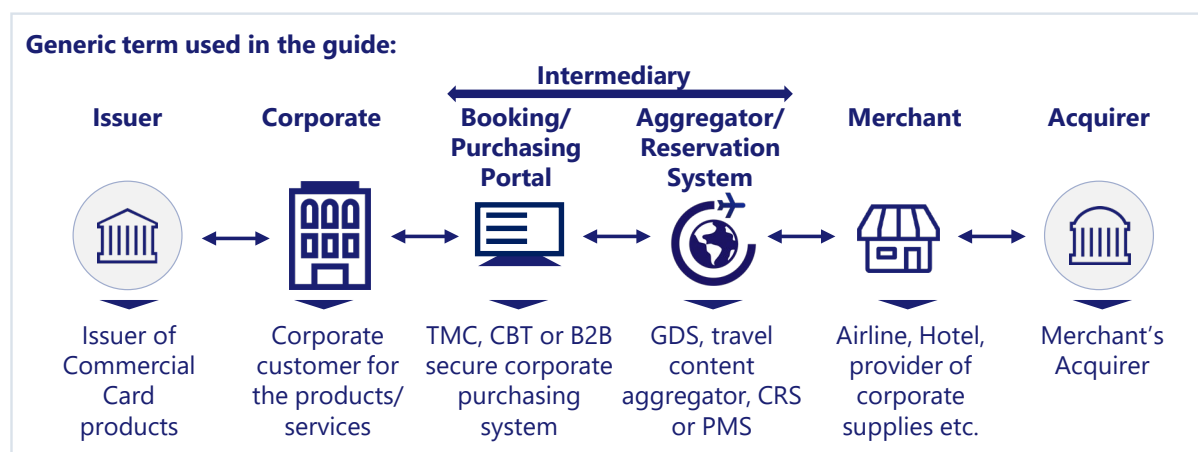
Examples include Global Distribution Systems (GDS), travel content aggregators, Customer Reservation Systems (CRS) & Property Management Systems (PMS).

- **Intermediary:** The term used to describe any party facilitating a transaction between a corporate and a merchant when it is not necessary to differentiate between the roles of a booking/purchasing portal and an aggregator. Includes one or more of TMCs, CBTs, purchasing portals, GDSs and content aggregators.

Where reference is made to a specific type of intermediary, the term for that specific type of intermediary is used, for example "TMC" or "GDS".

For definitions of the above ecosystem participants, please refer to the Glossary.

**Figure 1: The SCP payments ecosystem and generic terminology used in the guide**



## 3. Interpreting the regulation regarding the Secure Corporate Payment exemption

### 3.1 The key provisions of the regulation

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

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

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

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

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

### 3.2 Interpreting the exemption

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

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

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

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

### 3.2.2 Commercial card products to which the exemption may be applied

Visa considers that transactions made for business purchases using the following products used in the following ways could be within the scope of the exemption:

- Commercial virtual cards, CTAs, also referred to as lodged cards, or accounts that are “lodged” or embedded with B2B merchants<sup>2</sup>. These could include those used within an access-controlled corporate travel management or corporate purchasing system
- Physical Commercial Cards<sup>2</sup> that are issued for use by individual employees of a corporate entity when used within a secure corporate environment, may qualify for the exemption

### 3.2.3 Card products and use cases to which the exemption may not be applied

Personal cards that have been issued to an employee or contractor as a consumer do not qualify for the exemption, even if the transactions are for business purchases and transactions with those cards are initiated from within a secure corporate environment.

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

## 3.3 Examples of secure dedicated payment processes or protocols

Examples of secure corporate environments include:

- Corporate Travel Management Companies (TMCs) that store Commercial Card details of client employees within secure profiles that are only accessible by authorized employees through a secure log-in process
- Corporate travel booking tools (CBTs) that are only accessible by authorized employees through a secure log-in process<sup>3</sup>
- Corporate procurement systems that can be accessed by authorized employees through a secure log-in process

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

---

<sup>2</sup> For the Visa definitions of Commercial Card products and their allowable usage under Visa rules please refer to the definition of “Commercial Cards” and individual card types in the Glossary.

<sup>3</sup> Note corporate booking tools may in some cases be provided by T&H suppliers acting as merchants as well as by specialist CBT providers.



## 4. Applying the SCP exemption

---

### 4.1 Introduction to the use of the SCP exemption and the SCP exemption indicator

#### 4.1.1 Applicability of the SCP exemption

The SCP exemption is an Issuer applied exemption. It may be applied to qualifying transactions that are submitted either:

- Via EMV 3DS (the EMV 3DS flow) or
- Straight to authorization (the authorization flow)

As described in section 3.2.2 above, the SCP exemption may be applied to transactions made for business purchases using commercial virtual cards, CTAs and lodged cards, or to transactions made using physical Commercial Cards, where these transactions originate in a qualifying secure commercial environment as described in section 3.3.

#### 4.1.2 Issuer recognition of qualifying transactions & the SCP exemption indicator

Issuers of virtual cards, CTAs and lodged accounts can use the BIN or account ranges to recognise transactions made using these types of card product. All Commercial Card Issuers who support the SCP exemption (or their ACS when the transaction is submitted via the EMV 3DS flow) must check the BIN/account range for every transaction before taking a decision on application of the exemption or SCA to:

- Validate that the card being used is a qualifying Commercial Card that is not available to consumers
- Identify whether a qualifying virtual card, CTA or lodged account is being used

They should apply the exemption to all qualifying transactions made using these types of card product, where the relevant NCA is satisfied that the requirements of the regulation are met.

However, where a physical Commercial Card is used, Issuers cannot differentiate between transactions that originate within a secure corporate environment that qualifies for the exemption and transactions that originate in a public environment where SCA is required. Furthermore, it is often not possible to apply SCA to a transaction originating in a secure corporate environment such as a TMC, CBT or procurement system. This means that unless the Issuer is told that a transaction using a physical card qualifies for the exemption, the Issuer is likely to request SCA and the transaction may fail.

For this reason, Visa has made available an SCP exemption indicator that can be used by a merchant or their Acquirer, and in some cases an intermediary, for example a GDS, to flag to an Issuer that a transaction originates in a qualifying secure corporate environment and that it considers the SCP exemption may be applied. A version of the indicator is available in both F34 of the authorization request and in EMV 3DS, allowing the exemption to be flagged in both the authorization and EMV 3DS flows.

The indicator should only be set if the transaction has originated in a secure corporate environment that satisfies the requirements of the local NCA and that meets the requirements defined in section 4.7 and Appendix A.1.

### 4.1.3 The framework of the controls



Visa has also put in place a framework of controls<sup>4</sup> and is updating Visa rules to support the use of the SCP exemption indicator and require that it is only used to flag transactions that legitimately originated from environments that qualify for the application of the SCP exemption. Merchants/Acquirers may only submit transactions flagged with the SCP exemption indicator when they are satisfied that the requirements of the framework of controls have been met.

More detailed guidance on applying the SCP exemption, use of the SCP exemption indicator and the framework of controls is given in the following sections. For information on how fraud liability applies under the Visa rules when the SCP exemption is used please refer to Appendix A.2.

## 4.2 Applying the SCP exemption to transactions using different types of Commercial Card product

As described in section 3.2.2 the ability to apply the exemption depends on the type of Commercial Card and the environment in which the transaction originates. The applicability of the SCP exemption by card type and environment is summarized in Figure 2, and the requirements for use of the SCP indicator in the qualifying scenarios is described in more detail in sections 4.2.1, 4.2.2 and 4.2.3 below.

**Figure 2: Application of the SCP exemption to different Commercial Card types and environments**

To which card types can the SCP exemption be applied?		Physical Commercial Cards	Virtual Cards	CTA	Lodged Accounts
	Secure corporate environment	✓ SCP exemption indicator required	✓	✓	✓
	Public website	✗ SCA Required*	✓	N/A	N/A

\* Unless the transaction is out of scope of SCA or another exemption can be applied

### 4.2.1 Physical Commercial Cards

Merchants/Acquirers who wish to take advantage of the SCP exemption must use the SCP exemption indicator to flag qualifying transactions made using physical Commercial Cards if

<sup>4</sup> Note this framework of controls has been developed jointly by the major card schemes in consultation with Issuers, Acquirers and key stakeholders participating in a UK Finance working group dedicated to the application of the SCP exemption. The requirements apply to usage of the SCP exemption indicator across the EEA.

they would like the Issuer to apply the SCP exemption. If the indicator is not populated in such transactions, the exemption cannot be applied and SCA may be required by the Issuer if no other exemption can be used, which may cause the transaction to fail. Please refer to sections 4.4 and 4.5 for details of how to set the indicator.

#### 4.2.2 Commercial virtual cards, CTAs and lodged accounts

Use of the SCP exemption indicator by merchants, Acquirers or intermediaries to flag qualifying transactions made using virtual cards, CTAs and lodged accounts is optional, but recommended. However, it is recognised that merchants, Acquirers and intermediaries may not be able to identify that a transaction is made using one of these Commercial Card products. For this reason,

- The merchant, Acquirer or intermediary may populate the SCP indicator just like for physical Commercial Cards, or
- The merchant may not populate the indicator.

It is the responsibility of Issuers to identify and apply the exemption to qualifying transactions that use these Commercial Card products irrespective of whether the indicator has been set.

Visa rules require Issuers ensure dedicated account ranges within Commercial Card issuing BINs are used for Commercial Virtual Cards, CTAs and lodged accounts. Issuers of Commercial Card products that support the SCP exemption must therefore always check the account range/BIN for each transaction request they receive via EMV 3DS and/or authorization to determine whether the transaction may qualify for the exemption before requesting SCA.

#### 4.2.3 Use of the SCP exemption indicator by merchants/Acquirers when the card type is unknown

If a merchant, Acquirer or intermediary is unable to identify the card type used for a transaction originated in a qualifying secure corporate environment, it is recommended that they always set the SCP exemption indicator. They should however be aware that SCA may be required if the Issuer determines the card/transaction is not eligible for the SCP exemption, or for another Issuer applied exemption. If the transaction was sent direct to authorization, this means the merchant, Acquirer or intermediary may receive an SCA decline code<sup>5</sup>.

#### 4.3 Routing transactions with the SCP exemption indicator

In deciding whether to submit a potentially qualifying transaction straight to authorization or via EMV 3DS, the merchant or intermediary should consider:

- Its level of confidence that the card being used is eligible for the exemption, and
- Whether it will be possible to authenticate the cardholder should the Issuer refuse to support the exemption and request SCA at authorization.

If there is a possibility that the SCP exemption indicator will not be accepted by the Issuer and that the cardholder may be available to authenticate when the transaction is initially submitted

---

<sup>5</sup> For more details on the SCA decline code, which is used by an Issuer to request that a transaction sent to Authorization without SCA needs to be resubmitted with SCA, please refer to the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

but will not be available to authenticate at the time of authorization, it is recommended that the transaction is submitted via EMV 3DS.

#### 4.4 The SCP exemption via EMV 3DS

Issuers supporting the SCP exemption must inform their ACS when and how to apply it as follows:

##### 4.4.1 With the SCP exemption indicator

The 3DS Requestor (3DS Server) can indicate to the ACS that the SCP exemption may apply by populating the Authentication Request (AReq) with the 3DS Requestor Challenge Indicator (`threeDSRequestorChallengeInd`) = '82'. This is a specific value for Visa's EMV 3DS implementation which is defined as "No challenge requested (utilize Secure Corporate Exemption as applicable)". This value is accepted for all Visa EMV 3DS protocol versions.

The ACS response to the SCP exemption request will differ depending on the EMV 3DS protocol version in use:

- EMV 3DS 2.1.0: Authentication Response (ARes) message with Transaction Status (`transStatus`) = 'N', ECI value of '07', a CAVV and including a DS assigned Transaction Status Reason (`transStatusReason`) code = '89' (`CAVV_Included_In_Response`)
- EMV 3DS 2.2.0: Authentication Response (ARes) message with Transaction Status (`transStatus`) = 'I', an ECI value of '07' and a CAVV

For either protocol version, and in line with Visa mandates, it is recommended that the ACS generate a CAVV corresponding to Usage 3, Version 7 format (i.e. CAVV v7).

In the case of no response from the ACS or for non-participating ACS/Issuer, the Visa Attempts Server (AACS) will not acknowledge this exemption and will respond with a Transaction Status (`transStatus`) = 'N' and Transaction Status Reason (`transStatusReason`) = '87' – excluded from attempts.

If the SCP exemption was "requested" and accepted in the EMV 3DS flow, the merchant/intermediary/Acquirer must ensure they also populate the SCP indicator in the authorization flow.

If the Issuer does not support the exemption in general or for this particular transaction:

- A regular authentication flow can apply, that is a challenge can be requested and a Results Request (RReq) message with Transaction Status (`transStatus`) = "Y", CAVV and ECI 05 values returned if successfully authenticated or an "N" and an ECI value of "07" is returned if not successful, or
- The transaction can be declined directly by sending an Authentication Response (ARes) message with Transaction Status (`transStatus`) = 'N' and may also include an ECI with a value of '07'.

##### 4.4.2 Without the SCP indicator

Whenever the Issuer supports the SCP exemption, even if the SCP indicator is not present in the request, the ACS should always check the BIN/account range for every transaction before taking a decision on application of SCA or of any exemption. If the decision is to apply the SCP exemption, no challenge will be requested, and the ACS will respond with

- a Transaction Status (transStatus) = "Y", CAVV and an ECI value of 05.

#### 4.5 The SCP exemption indicator in authorization

The SCP exemption indicator is available in TLV Field 34 (Tag 88 in Dataset ID 4A) of the authorization message. It can be set for qualifying transactions by the merchant, Acquirer or intermediary by setting the values of Tag 88 as follows:

- 0 (SCA exemption does not apply to the transaction)
- 1 (Transaction exempt from SCA as the merchant/Acquirer has determined it as a secure corporate payment).

Note: If the SCP exemption does not apply to the transaction, the value of 0 is optional and the tag may be omitted entirely.

#### 4.6 Recognition of the indicator and application of the exemption by the Issuer

Issuers who support the SCP exemption will recognise the indicator and may choose to apply the exemption so long as the exemption is being requested for an eligible card.

If the Issuer decides not to apply the exemption to a transaction purely on the grounds that it considers that SCA is required,

- When indicated via the 3DS flow, it must apply a challenge
- When indicated in the authorization flow, it must either apply another exemption or respond with an SCA decline code to request resubmission with SCA.

##### 4.6.1 Minimising declines when SCA is not possible

When making authorization decisions, Issuers should consider that when the Acquirer has indicated that the transaction originates from a secure corporate environment, it may not be possible to authenticate an individual payer at the time of the transaction. They should therefore consider not using the SCA decline code to request SCA on transactions submitted straight to authorization, or initiate an SCA challenge for transactions submitted via 3DS, where the SCP exemption indicator is populated unless:

- Risk analysis indicates that the transaction is high risk or SCA is otherwise required, or
- The exemption is being requested for a transaction using an ineligible card product.

If the Issuer does request SCA there is a probability that the transaction will fail if the merchant or intermediary initiating the transaction is unable to support authentication.

#### 4.7 Frameworks of Controls & Visa requirements

The card payment schemes have worked with the travel and hospitality industry and industry associations (notably UK Finance) to develop a framework of controls to enable the SCP exemption to be applied to transactions originating in secure corporate environments other than secure payment processes such as virtual cards, CTAs and lodged accounts that are controlled directly by Issuers. The framework aims to ensure that the SCP exemption indicator is only used to flag transactions that originate in a qualifying secure environment. The framework, which is summarised in Figures 3 and 4 below, is underpinned by:

- Safeguards between stakeholders in the ecosystem, notably between Issuers and their corporate clients; Acquirers and merchants; merchants and intermediaries (such

as TMCs/CBTs, procurement systems and corporate marketplaces); and intermediaries and corporate customers. This is to ensure there is appropriate security and control throughout the ecosystem so the exemption may be applied appropriately

- Acquirer monitoring of the correct use of the SCP exemption indicator to ensure it is only being used by merchants who are entitled to do so, and only for transactions originating from qualifying secure environments
- Measurement of fraud rates by PSPs with remedial action being taken where fraud rates on transactions where the SCP exemption is used exceed TRA exemption fraud rates and/or increase.

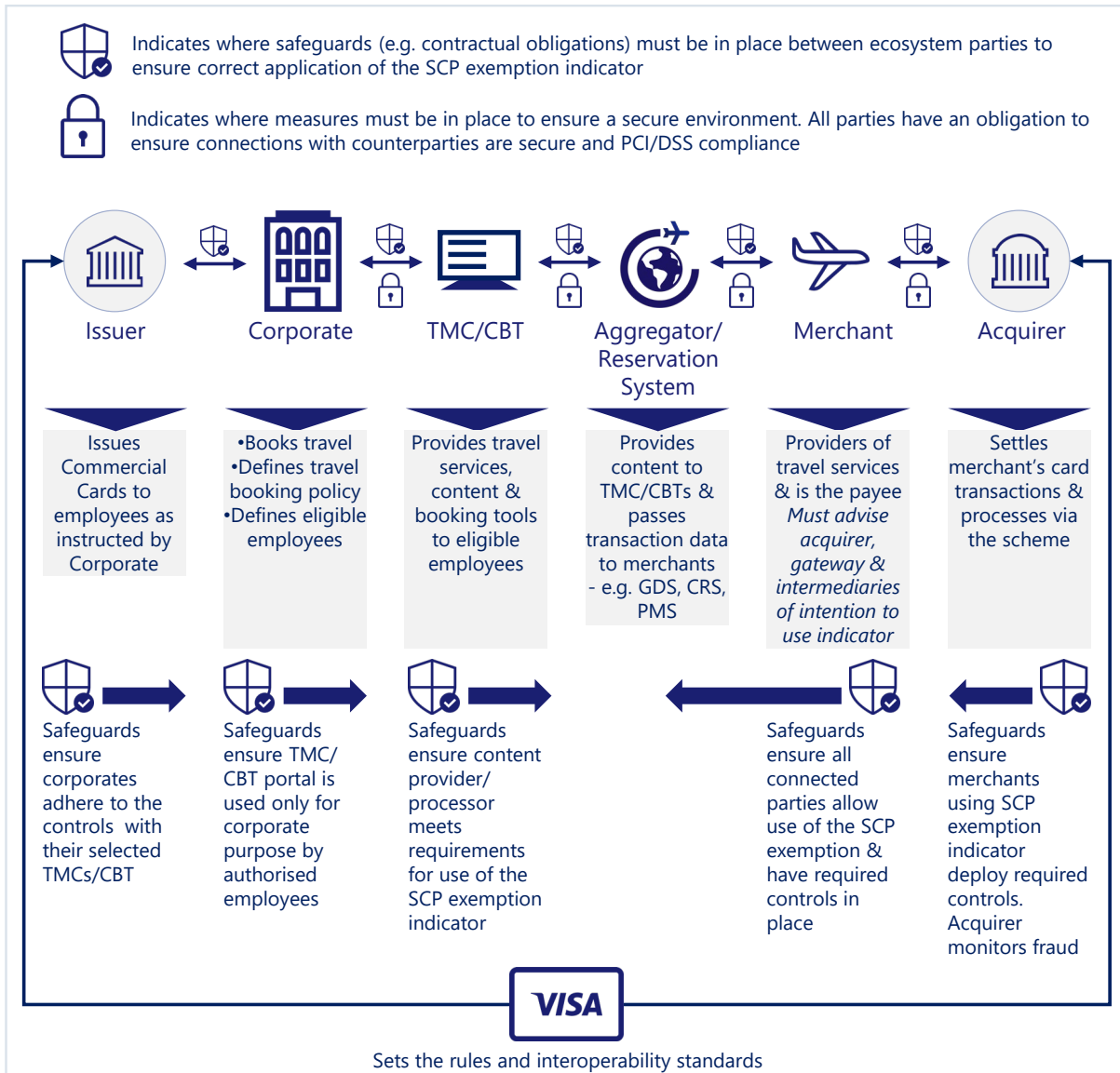
Visa Rules are being updated to include security conditions incorporated in the framework and these security conditions must be adhered to:

- When an Issuer enables its corporate customer to store its card on file with a TMC, CBT or in a procurement system
- When a merchant/Acquirer is to apply the SCP exemption indicator to a transaction originating from a secure corporate environment.

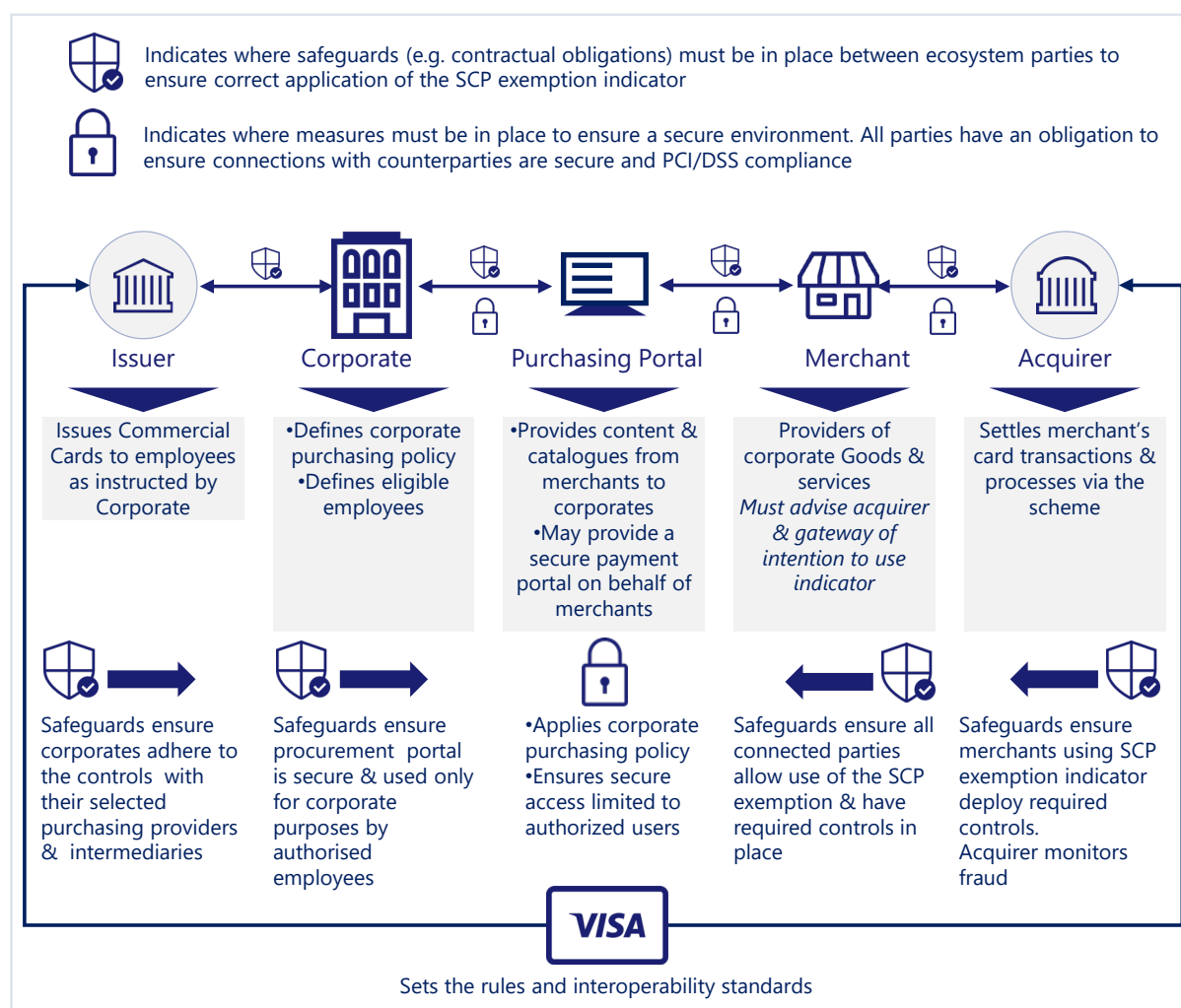
Adoption of the framework of controls between parties in the ecosystem is critical to ensuring that all stakeholders are able to correctly identify transactions originating from a secure corporate environment and which may qualify for the SCP exemption, and where transactions do not qualify to ensure that SCA can be applied and that transactions are not declined.

Visa's specific requirements for each stakeholder involved in the use of the indicator in the application of the exemption is summarised in Appendix A.1.

**Figure 3: Secure Corporate Payment Framework of Controls for corporate travel bookings**



**Figure 4: Secure Corporate Payment Framework of Controls for corporate purchasing**



## 5. Additional Impacts for Issuers

In addition to the requirements described in section 4 above, Issuers should take account of the following points to optimize the correct application of the SCP exemption and to minimise unnecessary Commercial Card transaction declines.

### 5.1 Demonstrating qualification to NCAs

Commercial card Issuers are encouraged to (and, for some NCAs, may be required to) demonstrate to NCAs that the relevant card products they issue and for which they intend to apply the exemption meet the requirements of the regulation and Visa recommends that Issuers liaise with NCAs over the procedure for this as required.

### 5.2 Supporting the SCP exemption indicator

Issuers supporting the exemption should ensure all their Commercial Cards, including virtual cards, CTAs and lodged accounts are enrolled in EMV 3DS<sup>6</sup> and should work with their ACS

<sup>6</sup> For more information on the reasons for this please see the *PSD2 SCA Commercial Cards Guide*



vendors to ensure that the SCP exemption indicator is supported in EMV 3DS, and must inform their ACS vendors of their policies as to when to agree to apply the exemption and which cards are eligible.

Issuers must ensure their authorization system also recognizes the SCP exemption indicator when transactions are submitted direct to authorization.

### 5.3 Meeting the requirements of the framework of controls

Issuers who support the SCP exemption are required to put in place with their corporate customers the safeguards defined by the framework of controls as summarised in Appendix A.1.

### 5.4 Encouraging the use of qualifying card products in secure corporate environments

Where an Issuer has registered their virtual card, CTA or lodged account products with an NCA and the NCA is satisfied that these products meet the requirements of the regulation for application of the SCP exemption, the Issuer may wish to encourage the use of these products for transactions originating in a secure environment (such as a TMC, CBT or corporate purchasing portal) to simplify the process of applying the exemption and reduce the risk that SCA may need to be applied.

Usage of these products instead of physical Commercial Cards where appropriate, enables the Issuer to apply the exemption without relying on the merchant/Acquirer to populate the SCP exemption indicator, and may provide more control.

### 5.5 Considering the use of other exemptions for non-qualifying Commercial Card transactions

There may also be an option to apply another exemption for transactions that do not qualify for the SCP exemption. For example, it may be possible to apply the TRA exemption, where transactions qualify, or the trusted beneficiaries exemption, where a corporate customer's transactions for goods or services are with known merchants that can be added to a cardholder's Trusted List. On this basis, Issuers should consider supporting the trusted beneficiaries exemption for Commercial Cards and offering this option for transactions that do not qualify for the SCP exemption<sup>7</sup>.

When Issuers receive a transaction using a Commercial Card product that they determine does not qualify for the exemption, they should seek to apply another qualifying exemption before requesting or applying SCA.

### 5.6 FCA requirements on Issuers (UK Only)

Issuers seeking to demonstrate qualification of a secure process or protocol for the exemption should also note that, in the UK, the FCA requires Issuers to:

- Provide comprehensive assessments of their operational and security risks, and the adequacy of mitigation measures and control mechanisms implemented in response to those risks. The secure payment processes or protocols need to be included in this assessment. PSPs intending to operate the exemption must provide the FCA

---

<sup>7</sup> It should be noted that SCA is required when a payee adds a new trusted beneficiary or amends their Trusted List. Accordingly, this will only be an option for Commercial Cards where SCA can be applied

with this information by including it in an assessment submitted at least 3 months before relying on the exemption.

- Ensure the process or protocol is subject to transaction monitoring (in line with SCA RTS Article 21), fraud prevention, security and encryption measures
- Ensure fraud rates are equivalent to, or lower than, the reference fraud rate for the same type of payment transaction as set out in the appendix to the SCA RTS.

### 5.7 The need to communicate with and support corporate customers

Issuers need to ensure that their Commercial Card customers fully understand the implications of the application of SCA and the SCP and other exemptions in the context of the purchasing processes used by those customers and encourage them to discuss those with their travel booking and procurement partners. This may include:

- Understanding that transactions may fail if SCA is required but a cardholder is unavailable to authenticate and an exemption cannot be applied. For example, if a physical card is used for a transaction initiated by a TMC and the cardholder is not available to authenticate at the time the booking is made
- Explaining the ways in which the Issuer supports the SCP exemption, for example through support of the SCP exemption indicator and/or the use of virtual cards, CTAs or lodged accounts for transactions originated in secure environments, and the circumstances where SCA may not be required
- Describing the requirement for corporate customers to put in place the required safeguards with their purchasing partners including TMCs, CBTs, procurement systems and B2B merchants if the SCP exemption indicator is to be used, as defined in the framework of controls
- Discussing changes to business practices and purchasing processes that they may need to make to prevent transactions failing. For example, ensuring that the SCP exemption indicator can be set by the end merchant, or ensuring that virtual cards, CTAs or lodged accounts are used rather than physical cards in environments where SCA cannot be applied.
- Guiding the customer's choice of Commercial Card products in order to facilitate the application of the SCP exemption and prevent declined authorizations.

Additional guidance on best practices for the use of Commercial Cards in the context of PSD2 SCA are included in the *PSD2 SCA Commercial Cards Guide*

## 6. Additional impacts for Acquirers

---

### 6.1 Supporting merchants with the use of the SCP exemption indicator

Acquirers must be able to explain the impacts of SCA to merchants who accept bookings and purchases that are made using Commercial Cards and originate in a secure corporate environment, and the potential there is to indicate to Issuers that the SCP exemption may apply. When the exemption may apply, they must be ready to support the SCP exemption indicator and explain how the indicator must be used as explained in this guide. They should

work with merchants who are able to make use of the indicator to ensure that it is supported in their EMV 3DS implementation and/or authorization requests.

Acquirers must also inform these merchants that transactions with the SCP exemption indicator set in EMV 3DS are excluded from Visa Attempts Server processing. This means if the Issuer's ACS fails to respond due to a technical issue (or for non-participating ACS/Issuer i.e. no ACS URL) the Visa Attempts Server will step in and return with:

- 'N' (Not Authenticated/Transaction Denied)
- Transaction Status Reason Code of '87' (excluded from attempts)

Merchants must be advised that upon receiving such a response, they may try to submit the transaction direct to authorization with the SCP exemption indicator for the Issuer to apply the SCP exemption direct at authorization.

## 6.2 Meeting Visa's framework of controls requirements for use of the SCP exemption indicator

Acquirers must ensure that where they submit the SCP exemption indicator in an authorization request, the requirements of the framework of controls are met, including having the required safeguards in place with their merchants. These requirements are summarized in Appendix A.1.

# 7. Additional impacts for merchants & intermediaries processing transactions on behalf of merchants

---

In addition to the requirements described in section 4 above, merchants and intermediaries should take account of the following points to ensure the SCP exemption is only requested for qualifying transactions and to minimise unnecessary Commercial Card transaction declines.

## 7.1 Merchant use of the SCP exemption indicator

Qualifying merchants (or intermediaries who process on their behalf, for example GDSs) who process transactions originating from secure corporate purchasing systems or travel management systems should discuss with their Acquirer to determine whether any of their transactions should/could be flagged using the SCP exemption indicator in EMV 3DS and/or in the authorization message. This enables a transaction to be processed without authentication, so long as the Issuer supports the exemption and the card is eligible for it.

Consideration should be given as to whether to submit transactions flagged with the indicator straight to authorization or via EMV 3DS, as described in section 4.3.

In order to apply the exemption using the SCP exemption indicator, merchants must also:

### 7.1.1 Be able to identify and flag transactions originating from a qualifying secure corporate environment

A merchant (or an intermediary processing on its behalf such as a GDS) accepting transactions from third party channels that initiate purchases using a secure corporate environment must ensure that it can recognise that the transaction originated in a qualifying environment and that it can set the SCP exemption indicator when submitting the transaction to authorization. For example, a travel and hospitality sector merchant accepting a transaction originated by a TMC must be able to recognize that the transaction originated via a secure environment, regardless of whether it received the transaction directly via an API or via an aggregator/reservation system.

Merchants should note they can only set the indicator if they are certain the transaction originates from a secure corporate environment. This means the SCP exemption cannot be applied, and the indicator cannot be set if:

- The transaction originates from a public website, (including travel bookings made via TMCs/Aggregators using screen scraping), or from
- Another booking agent or channel that does not meet the requirements of the NCA for the application of the SCP exemption.

This applies to transactions received directly from the booking agent/procurement system or received via an intermediary or aggregator.

The impact is that the merchant will not be able to set the SCP exemption indicator for any transactions where they cannot be certain the controls required in Appendix A.1 have been met. Where this is the case, they will have to ensure SCA is applied, unless the transaction qualifies for another exemption or is out of scope.

Merchants must be aware that even if the transaction originated in a qualifying secure environment, if the Issuer determines that the card used was not eligible for the SCP exemption or the transaction carries a high fraud risk, the Issuer may:

- Request a challenge, if the transaction is submitted via EMV 3DS, or
- Respond with an SCA decline code, requesting resubmission with SCA, if the transaction is submitted straight to authorization.

Merchants and any third party booking or purchasing systems or intermediaries they receive transactions from, should agree strategies for routing and flagging qualifying transactions. These should include specifically agreeing under what circumstances transactions flagged with the SCP exemption indicator should be submitted via EMV 3DS and when they should be sent straight to authorization. For more information please see section 4.3.

### 7.1.2 Meet the requirements of the Framework of Controls

In order to use the SCP exemption indicator for transactions originating through third party channels, merchants (or their processors such as GDSs) must ensure that the requirements defined by the framework of controls are met. These requirements are summarized in Appendix A.1.

## 7.2 Impacts on intermediaries processing bookings or orders on behalf of merchants

### 7.2.1 Passing of authentication and payment data to support the application of the SCP exemption indicator

Where bookings or orders originated via a TMC/CBT or a procurement system are sent via a GDS or another aggregator/reservation system (other than the merchant) and the SCP exemption is to be used:

- In the case of a GDS, the GDS will request authorization via VisaNet, on behalf of the merchant, by populating the SCP indicator in the authorization request and submitting it. If the transaction has been submitted via EMV 3DS, the authentication data must be submitted with the authorization request.
- In the case of another aggregator/reservation system, the aggregator/reservation system must pass to the merchant or its Acquirer, data indicating the SCP exemption is being requested, along with the authentication data if the transaction has been submitted via EMV 3DS, so the merchant or the merchant's Acquirer can include the SCP indicator and authentication data (when available) in the authorization request

See section 8.1 for more detailed example explanations of these flows.

Solution providers and intermediaries must be able to receive and pass specific authentication data<sup>8</sup> and/or the SCP exemption indicator (or other information indicating that the SCP exemption is being requested) along with associated payment data to merchants and/or Acquirers and/or Schemes following an indirect booking or order. This will require that intermediaries that pass information associated with transactions originated via TMCs, CBTs and other procurement systems work together to agree a proprietary, secure process for passing this data. If the SCP exemption indicator is to be used, this process should meet the requirements of the framework of controls as summarised in Appendix A.1.

Note that these requirements apply where transactions use physical Commercial Cards, and the SCP exemption indicator must be set if the SCP exemption is to be applied. They may not apply where transactions exclusively use virtual cards, CTAs or lodged accounts and the use of the SCP exemption indicator is optional and may not always be used.

Example use cases illustrating the high level flows are included in section 8.

### 7.2.2 Meeting the requirements of the framework of controls

All intermediaries should take steps to ensure that only qualifying transactions are submitted with the SCP exemption indicator.

### 7.2.3 Specific impacts on booking/purchasing portals

In the case of transactions carried out with non-qualifying cards, booking and purchasing portals must ensure that the cardholder is able to complete an SCA challenge where this is required at time of booking or placing an order. This requires the portal to establish processes with customers to take account of the potential need to apply SCA, or to exclude non-qualifying cards from their processes, and to ensure that the requirements of the framework of controls as summarised in Appendix A.1 are met.

---

<sup>8</sup> The data that needs to be passed is defined in Appendix A.3 of *Implementing Strong Customer Authentication (SCA) for Travel & Hospitality V2.0*.

If portals wish to continue to support non qualifying cards within their systems, they will need to ensure that transactions can be authenticated, including the ability to contact the cardholder to authenticate a transaction in the case that an SCA decline code is received from the Issuer.

## 8. Example Use cases

---

The following are examples of B2B use cases where the SCP exemption may be applicable:

### 8.1 Corporate travel booking made via a TMC/CBT

#### 8.1.1 Qualification criteria

In this use case, it is assumed that the booking transaction is made using either:

- A physical Commercial Card issued to an employee of a qualifying corporate customer, where the requirements of the exemption are otherwise met, and the NCA has been advised of the intention to use the SCP exemption, or
- A virtual card or CTA product that has been registered with the NCA by the Issuer and the NCA is satisfied that the conditions of the regulation are met. If any of these conditions do not apply, the SCP exemption cannot be applied and, unless the transaction qualifies for another exemption, it must be submitted for authentication, or an alternative card used.

#### 8.1.2 Transaction initiation via the TMC/CBT

There are three potential scenarios for submission of the transaction by the TMC/CBT:

##### **Scenario 1: submission via a GDS and the role of the GDS**

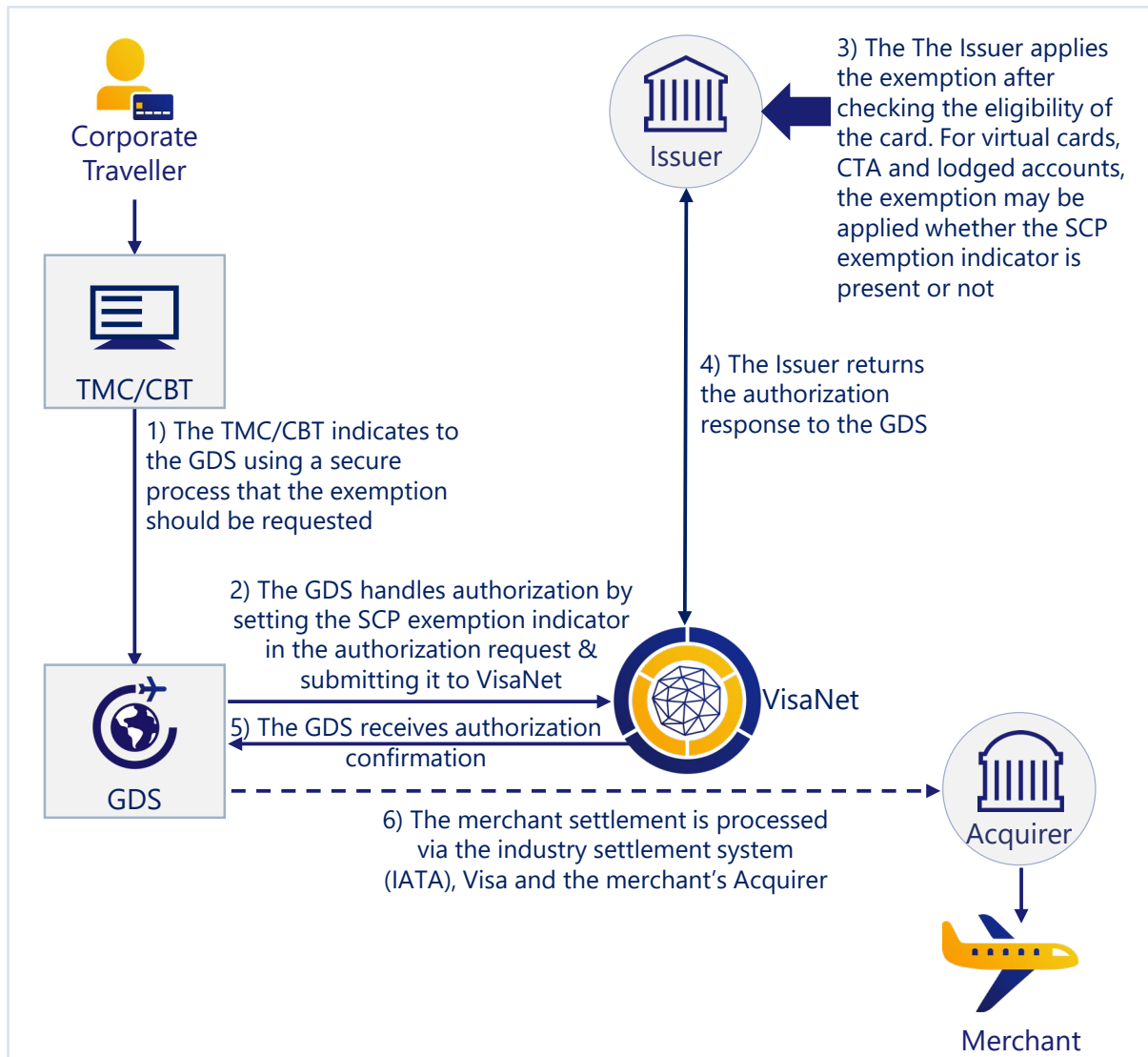
If the TMC/CBT submits the booking directly to the GDS, the transaction authorization request is routed direct to VisaNet). Where the transaction is made using a physical card, the TMC/CBT should indicate to the GDS that the transaction qualifies for the SCP exemption and the GDS should populate the SCP exemption indicator in F34 to ensure that the transaction is not declined. It is also recommended that the indicator is populated in the same way if the transaction is made using a virtual card or CTA, so long as the TMC/CBT supports the indicator and is able to recognize that one of these card products has been used. Please note that the GDS can only populate this indicator if it is certain the transaction originates from an environment that meets the conditions required by the regulation and the framework of controls and it should have safeguards in place to ensure this is the case.

Alternatively, the TMC/CBT may submit the transaction via EMV 3DS before authorization is requested, in which case the SCP exemption indicator needs to be set in the EMV 3DS request. The GDS must then be provided with the CAVV and associated ECI value obtained during the authentication request and be informed that the SCP exemption is being used. The GDS must set the SCP exemption indicator in the authorization request and include the authentication data.

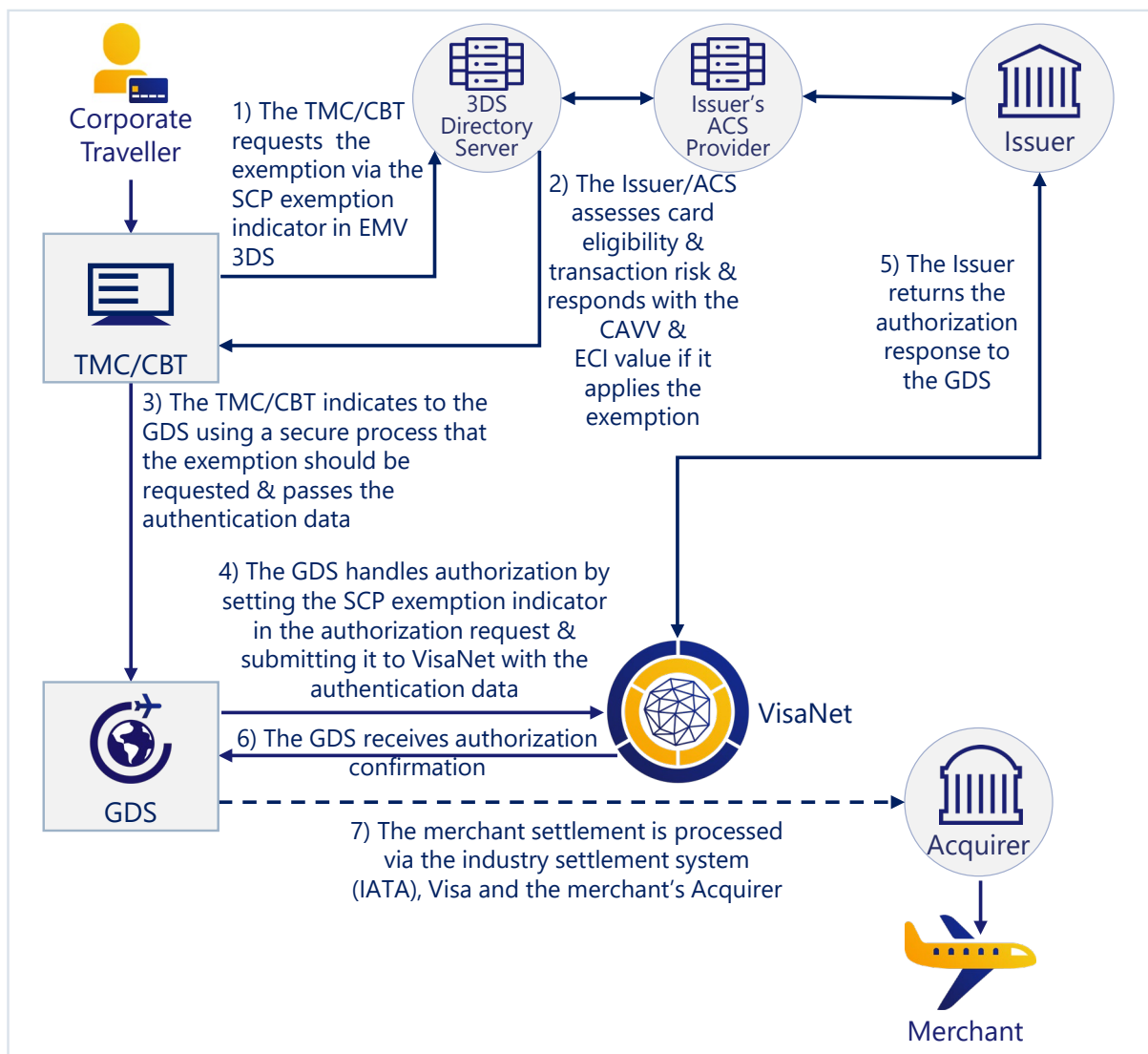
Once the transaction is authorized, the merchant settlement is processed via the industry settlement system (IATA), Visa and the merchant's Acquirer.

The straight to authorization and EMV 3DS flows are summarised in Figures 5 & 6 below:

**Figure 5: Transaction submitted via GDS – SCP exemption indicated via authorization flow**



**Figure 6: Transaction submitted via GDS – SCP exemption indicated via EMV 3DS flow**



### Scenario 2: submission direct to the merchant and the role of the merchant

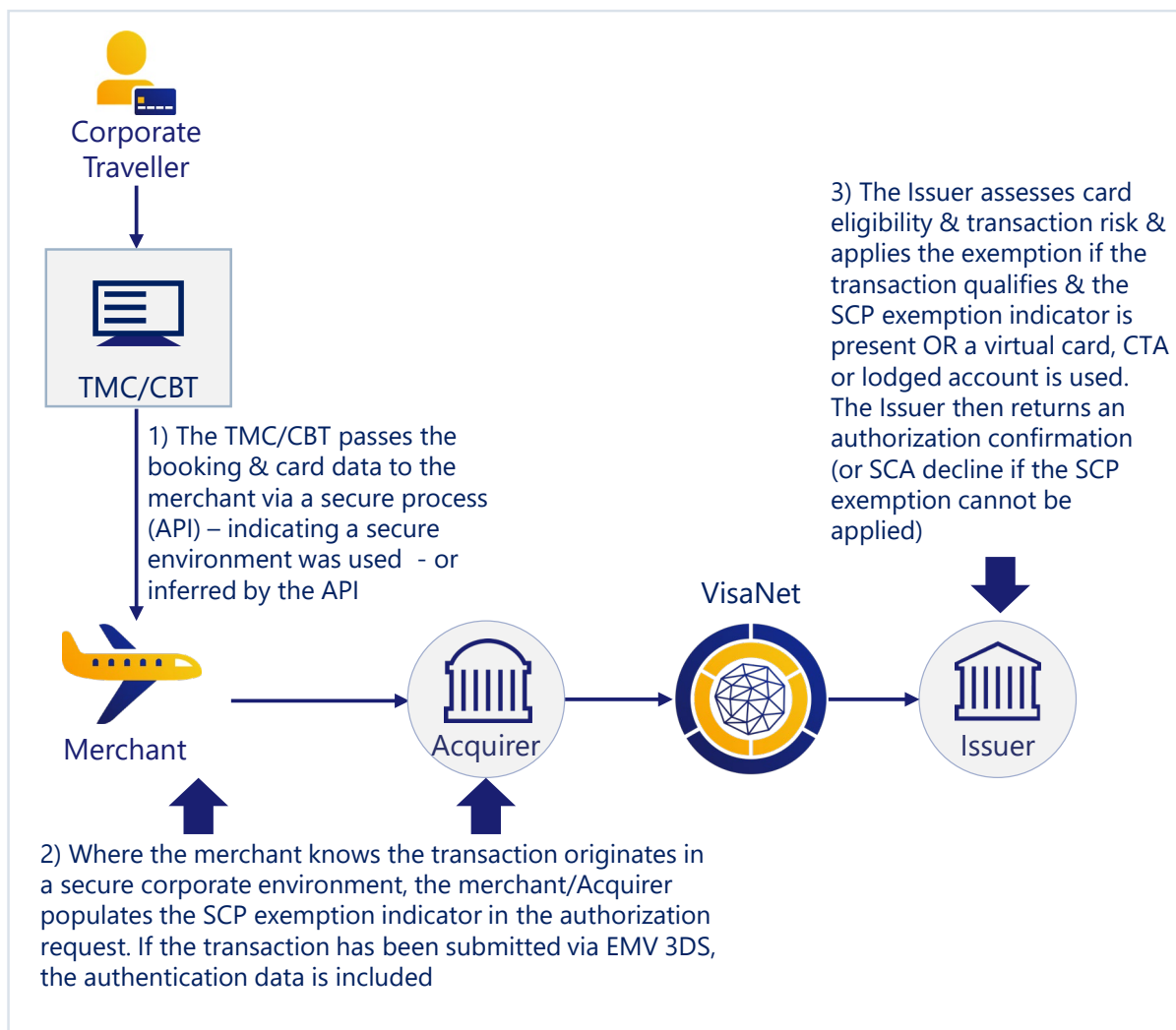
Alternatively, TMCs/CBTs and procurement system aggregators can integrate directly with the merchant via a secure API, as shown in the example in Figure 7 below. In this case, the merchant can recognise that the transaction has originated in a qualifying secure TMC/CBT/procurement environment and should submit the transaction straight to authorization with the SCP exemption indicator populated (and with CAVV and associated ECI value, if any is received).

The TMC/CBT/procurement system also has the option to submit the transaction via EMV 3DS before authorization is requested, in which case the SCP exemption indicator needs to be set in the EMV 3DS request. The merchant must then be provided with the CAVV and associated ECI value obtained during the authentication request and be informed that the SCP exemption is being used. The merchant must set the SCP exemption indicator in the authorization request and include the authentication data.

Note that TMCs, CBTs and other intermediaries should not place bookings using a physical Commercial Card via a merchant's public website (including through screen scraping) if they would like the SCP exemption to apply. These transactions do not qualify for the exemption.



**Figure 7: Submission direct to merchant**



### Scenario 3: TMC is the merchant for billing their own services

In this scenario, the TMC is the merchant billing fees for their own travel services, or for bill-backs where they are recharging the corporate customer for a booking made by the TMC using another payment method. These transactions are submitted directly via the TMC's Acquirer. In this case, as the TMC is the merchant, it must indicate to the Acquirer that the transaction originates in a secure environment. So long as the safeguards in the framework of controls are correctly applied, the Acquirer can populate the SCP exemption indicator in F34 of the authorization message. Please refer to section 8.2 for an illustrative example of how an agent subsequently pays a supplier when it has acted as the merchant in collection of payment from the end customer.

#### 8.1.3 Issuer response

In any of the above scenarios, when the Issuer receives the transaction with the SCP exemption indicator set, they should consider applying the SCP exemption unless:

- The Issuer determines the transaction is high risk or SCA is otherwise required, in which case it should apply SCA if the transaction has been submitted via 3DS or issue an SCA decline code requesting that the transaction is resubmitted for authentication via 3DS

- The Issuer determines that the transaction does not qualify for the exemption, in which case the Issuer should:
  - Check whether an alternative Issuer exemption can be applied
  - If the transaction does not qualify for an alternative exemption either apply SCA or issue an SCA decline code requesting that the transaction is resubmitted for authentication. Note that this may result in the transaction being lost if SCA cannot be applied.

## 8.2 Travel booking B2B payment between an online travel agent & supplier using a virtual card

An Online Travel Agent (OTA)<sup>9</sup> may use virtual cards to complete a booking and subsequently pay a travel or hospitality supplier on behalf of a consumer. In this case, the OTA acts as the merchant and processes the consumer's payment, via its own Acquirer, charging the consumer's card accordingly. The OTA subsequently pays the individual supplier merchants (e.g. airlines, hotels etc.) through B2B payments originating in the OTA's secure B2B payment environment and using virtual cards.

Subject to the opinion of the NCA, these B2B virtual card based transactions would be eligible for the SCP exemption. This approach enables an OTA to complete a PSD2 compliant booking with multiple merchants without the need to use 3DS 3RI to obtain authentication data for each merchant<sup>10</sup>. However, please note that this requires the OTA and the supplier to operate an appropriate business model. The B2B payment transaction may take place directly between the OTA and the merchant or via a GDS as illustrated in Figure 8.

In this case, as the supplier settlement payment is made using a virtual card, use of the SCP exemption indicator is optional, but recommended, even where the supplier payment transaction is performed via a GDS. However, please note that the GDS will need to be aware the transaction is made using a virtual card to use the SCP exemption indicator. If the SCP exemption indicator is used, the OTA must indicate this to the GDS via the proprietary interface between the OTA and the GDS.

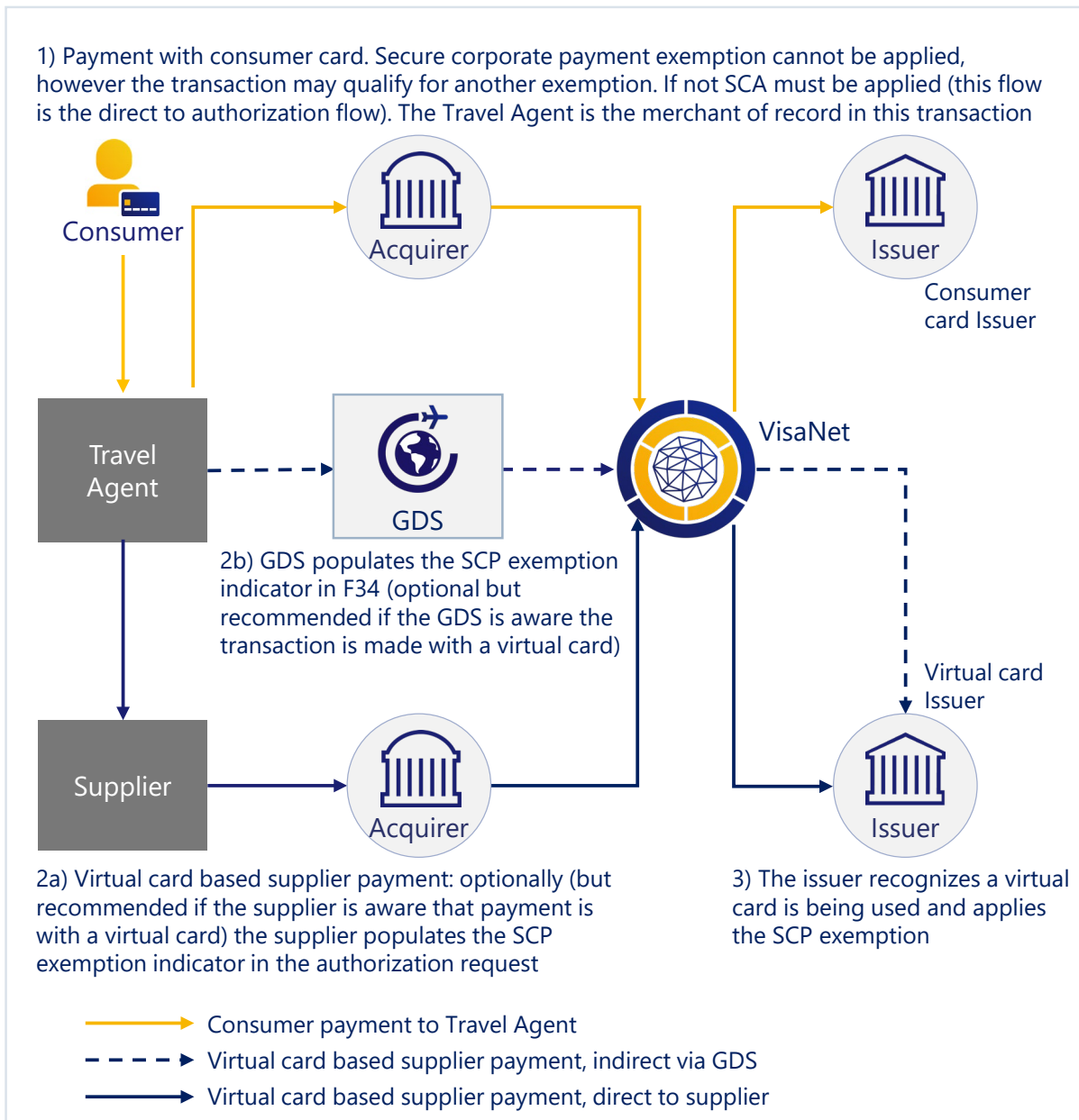
Note: The only time an Online or face-to-face Travel Agent can use the SCP exemption is when paying with their own virtual card. Physical Commercial Cards used in a consumer environment are still subject to SCA requirements.

---

<sup>9</sup> A similar model may also be used by some TMCs.

<sup>10</sup> Please refer to *Implementing Strong Customer Authentication (SCA) for Travel & Hospitality V2.0* for more details

**Figure 8: OTA to supplier virtual card payment**



## 9. Bibliography

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

**Table1: Bibliography**

Document/Resource	Version/Date	Description
COMMISSION DELEGATED REGULATION (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication	13 March 2018	The PSD2 Regulatory Technical Standards (RTS) published by the European Banking Authority (EBA) that establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to comply with the security requirements of the PSD2 legislation.
Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC	EBA-Op-2018-04 13 June 2018	EBA opinion paper clarifying various RTS requirements notably on the application of exemptions
EBA Q&A		EBA Online Q&A Tool that provides answers to specific questions raised by interested stakeholders. This is available at <a href="https://eba.europa.eu/single-rule-book-qa/qna/view/publicId">https://eba.europa.eu/single-rule-book-qa/qna/view/publicId</a>
PSD2 SCA for Remote Electronic Transactions Implementation Guide	Version 3.0 Jan 2021	Comprehensive Implementation Guide providing practical guidance on implementing SCA and Visa solutions.
PSD2 SCA Regulatory Guide	Version 1.0 December 2020	Summarises the main requirements of the PSD2 SCA regulation as it applies to electronic card payments and Visa's guidance on the practical application of SCA in a PSD2 environment.  The guide aims to provide a clear single point of reference providing guidance on interpreting the regulation.

PSD2 SCA Commercial Cards Guide	Version 1.1 March 2021	Provides Issuers of Commercial Cards with guidelines on the application of SCA and the other exemptions defined in the PSD2 SCA RTS to remote electronic transactions performed with Commercial Cards. It also summarises guidance that Issuers may wish to give to their Commercial Card customers to ensure that transactions are not unnecessarily declined due to the inability to apply SCA.
Implementing Strong Customer Authentication (SCA) for Travel & Hospitality	Version 2.0 June 2021	Provides specific guidance to T&H merchants, booking agents and intermediaries and to Issuers, Acquirers and gateways on the application of SCA to sector specific booking and payment scenarios
PSD2 SCA Optimisation Best Practice guide	July 2020	This guide provides merchants, Acquirers and Issuers with guidance on minimising the number of transactions that will require Issuers to apply SCA challenges.
PSD2 SCA Challenge Design Best Practice Guide	July 2020	This guide provides merchants, Acquirers and Issuers with guidance on minimising friction when SCA challenges are required.
PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements	Version 2.0 December 2020	Guide summarizing Visa Rules relevant to the application of PSD2 SCA.
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>

## 10. Glossary

**Table 2: 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>The current version of 3DS is referred to as EMV 3DS. Two version of the EMV 3DS specification are currently deployed EMV 3DS 2.1 and EMV 3DS 2.2. EMV 3DS 2.2 is required to fully support PSD2 SCA indicators.</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>
A	
Authentication	Authentication allows the Issuer to verify the identity of the cardholder or the validity of the use of the card, including the use of the cardholder's personalized security credentials and, where required, takes place before authorization, using the Issuer's selected authentication method, which in most cases will be 3-D Secure
Authorization	Authorization determines if a specific transaction request receives an approval or a decline from the issuing bank, or from VisaNet standing in on the issuing bank's behalf. Once a cardholder initiates a purchase, VisaNet informs the Issuer of the transaction, and receives back their approval or decline response. VisaNet then informs the requestor of the response, who passes the information along to the Merchant.
C	
Central Travel Account (CTA) or Lodged Account (sometimes also referred to as "Ghost Cards")	<p>A card account that is issued to a corporate customer (a company or organization), not an individual, and is typically:</p> <ul style="list-style-type: none"> <li>• Held by an agent, such as a Travel Management Company (TMC), approved by the corporate customer to make</li> </ul>

Term	Description
	<p>authorised travel purchases or bookings on behalf of the corporate customer, or:</p> <ul style="list-style-type: none"> <li>• Lodged/embedded directly with a merchant by the corporate customer and used by the merchant to charge for agreed goods and services ordered by the customer</li> </ul> <p>No physical card is issued.</p> <p>The CTA 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.</p>
Corporate Booking Tool (CBT)	A secure software system used by corporates to enable authorized employees to make corporate travel bookings
Commercial Card	<p>A Visa Card issued to a Client Organization for business-related purchases, as specified in the Visa Rules, and associated with an Issuing BIN, account range, or an account designated as one of the following Visa product types:</p> <ul style="list-style-type: none"> <li>• Visa Corporate Card (credit/deferred debit)</li> <li>• Visa Business Card (debit and credit/deferred debit)</li> <li>• Visa Purchasing Card (credit/deferred debit)</li> </ul> <p>These product types may be issued as physical cards, virtual cards, Central Travel Accounts (not Visa Business Cards) or lodged accounts (see the definition of these card and account types in this Glossary).</p>
Customer Reservation System (CRS)	Software platform or system that connects hotels and other travel & hospitality suppliers to TMCs, travel agents and online booking sites, enabling the supplier to receive and manage reservations
<b>E</b>	
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 include:</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>
<b>G</b>	

Term	Description
Global Distribution System (GDS)	An entity that aggregates and distributes flight schedule and ticket data and booking processes between airlines, travel agents, TMCs and CBTs and authorizes card transactions on behalf of merchants. May also aggregate data and bookings for hotels and other travel service suppliers.
<b>L</b>	
Lodged Account	See Central Travel Account (CTA) and Lodged Accounts
<b>P</b>	
Physical Commercial Cards	Physical credit or debit cards issued to an individual named cardholder for business expenditure. These cards are sometimes referred to as "walking plastic"
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.
Procurement Systems	Secure software systems or processes used by corporates to enable authorized employees to procure approved non-travel related goods and services, including through catalogues, marketplaces or approved supplier listings.
Property Management System	Software platform or system that connects hotels to TMCs, travel agents and online booking sites, enabling the hotel to receive and manage reservations and manage the day-to-day operations of the hotel property
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>11</sup> .

<sup>11</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) for e-commerce. Merchants and PSPs should check with NCAs for enforcement timescales in their respective markets.



Term	Description
PSP	In the context of PSD2, Regulated PSPs are responsible for the application of SCA and of the exemptions. In the case of card payments, these PSPs are Issuers (the payer's PSP) or Acquirers (the payee's PSP).
<b>R</b>	
Regulatory Technical Standards (RTS)	<p>An RTS is a standard that supplements an EU directive. An RTS is developed for the European Commission, in the case of PSD2 by the European Banking Authority (EBA) and is then adopted by the Commission by means of a delegated act.</p> <p>The PSD2 SCA RTS, (formally titled <i>Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication</i>) establishes the requirements to be complied with by payment service providers for the purpose of implementing security measures which enable them to comply with the security requirements of the PSD2 legislation.</p>
<b>S</b>	
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.
SCA decline code	A decline code (Response code 1A) used by an Issuer to request that a transaction sent to Authorization without SCA needs to be resubmitted with SCA. This process is also sometimes referred to as a "soft decline".
<b>T</b>	
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.

Term	Description
Travel Management Company (TMC)	A travel booking agent exclusively making travel bookings on behalf of contracted corporate customers.
Trusted Beneficiaries Exemption	An exemption defined in the PSD2 RTS that allows, subject to certain restrictions, that a payer may add a trusted merchant to a list of trusted beneficiaries (Trusted List) held by their Issuer, completing an SCA challenge in the process. Sometimes referred to as "whitelisting".
<b>V</b>	
Virtual Card	<p>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.</p> <p>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.</p> <p>Please note that "virtual card" is a general term that may include either real card numbers (PANs) or tokens. In either case the virtual card use case is focused on the temporary nature of the card, the controls and security that surround its usage and the absence of a cardholder to authenticate.</p> <p>Virtual Commercial 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. Three examples are:</p> <ul style="list-style-type: none"> <li>• Travel agencies settling booking payments with hotels,</li> <li>• Delivering virtual cards to employee's mobile device to enable them to pay for an urgent expense when they don't have a card of their own, and</li> <li>• Corporates paying a supplier for an invoiced amount for goods/services rendered.</li> </ul>
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.

# A Appendices

## A.1 Framework of Controls & Visa requirements

The following controls should be applied between ecosystem participants to enable application of the SCP exemption, and safeguard against abuse: Please refer to Figures 3 & 4 in Section 4.7 for a summary of the role of each the parties listed in Table 3 below.

**Table 3: Visa requirements on the parties in the ecosystem for the use of the SCP exemption indicator**

Party	Requirement related to the use of the secure corporate payment exemption - from enforcement date
<b>1) Issuers</b>	Issuers are required to <ul style="list-style-type: none"> <li>• Have in place appropriate safeguards (e.g. contractual agreement) with their Corporate requiring them to meet the obligations on Corporates listed in item 2)</li> </ul>
<b>2) Corporates</b>	Must have appropriate safeguards (e.g. a contractual agreement) in place with entities operating a travel booking/B2B purchasing portal for the usage of the Corporate's employees to ensure the requirements (listed below under item 5.1) are met
<b>3) Acquirers (or GDS connecting to Visa to process on behalf of a merchant that has a contract with the applicable Acquirer)</b>	<p>Acquirers are required to</p> <ul style="list-style-type: none"> <li>• Have in place safeguards with their merchants that are permitted to use the SCP exemption indicator confirming the below requirements for merchants in item 4) have been met</li> <li>• Ensure that all transactions sent to Visa with the SCP exemption indicator meet the below obligations placed on the merchant in item 4)</li> <li>• Monitor quarterly fraud rates on transactions with the SCP exemption indicator and inform Visa of any merchants with fraud higher than the relevant TRA exemption fraud thresholds on SCP indicated transactions</li> </ul> <p>Acquirers can only submit transactions with an SCP exemption indicator when a transaction originated:</p> <ul style="list-style-type: none"> <li>• From a merchant entitled to use the indicator and</li> <li>• Where the merchant can confirm the transaction originated from a secure corporate environment that meets requirements listed below either under item 5.1) or under item 6)</li> </ul>
<b>4) Merchants (or GDS processing on their behalf)</b>	Merchants eligible to use the SCP exemption indicator, as per rules agreed with their Acquirer, must put appropriate safeguards (e.g. a contractual agreement) in place with entities operating a corporate booking portal or, when there is no direct relationship with such entities, with the entities connecting them to a secure corporate tool/portal confirming that the below first set of requirements for these entities have been met

	<p>Merchants can only populate the SCP exemption indicator when:</p> <ul style="list-style-type: none"> <li>• They can confirm the transaction originated from an environment that was secure as per the below requirements for entities operating a travel corporate booking/B2B purchasing portal (item 5.2), and for Entities connecting a merchant to a corporate booking/B2B purchasing portal (item 6) where applicable.</li> <li>• There is a recognisable and Secure electronic connection between <ul style="list-style-type: none"> <li>• the merchant and the entity operating the travel booking/B2B purchasing portal (in case of a direct connection) or</li> <li>• between the merchant and the entity connecting the merchant with a travel booking/B2B purchasing portal and between this entity(ies) and the portal (in case of an indirect connection)</li> </ul> </li> </ul>
<p><b>5) Entities operating a travel corporate booking/B2B purchasing portal</b></p>	<p>5.1) These entities are required, by their Corporate partner, to ensure the corporate portal:</p> <ul style="list-style-type: none"> <li>• Can only be used for: <ul style="list-style-type: none"> <li>• corporate purposes</li> <li>• by permitted users (corporate employees)</li> </ul> </li> <li>• Must be protected by access controls with a level of security which meets PSD2 requirement</li> <li>• Must be connected to a merchant that will use the SCP exemption via a secure electronic connection (directly or indirectly via intermediaries)</li> </ul> <p>5.2) These entities are required, by their merchant partner (or other entities in between them and the merchant) to ensure the corporate portal meets at a minimum the following:</p> <ul style="list-style-type: none"> <li>• Clearly displays Terms and Conditions of the purchase or booking to the cardholder, including if transactions are to be later initiated by the merchant (MIT)</li> <li>• PCI-DSS certification</li> <li>• GDPR compliance</li> <li>• Secure access control</li> <li>• Is connected to the merchant (or any entities in between the portal and the merchant) via a secure electronic connection</li> </ul>
<p><b>6) Entities connecting a merchant to a travel corporate booking/B2B purchasing portal</b></p>	<p>These entities must:</p> <ul style="list-style-type: none"> <li>• Ensure the corporate portal they are connected to and from whom they send transactions for which the merchant is expected to use the SCP exemption indicator meets the requirements placed on those entities listed above</li> <li>• Be connected to both the entity operating a portal and to the merchant receiving bookings eligible to use the SCP exemption indicator via a secure electronic connection</li> </ul>

## A.2 Appendix 2 –SCP exemption fraud liability table

Table 4 below summarises how liabilities for fraud-related chargeback liabilities apply between the Issuer and the Acquirer under the Visa Rules when the SCP exemption is used.

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

Please note that that disputes liability under the Visa Rules may differ from “regulatory liability” under PSD2. If a merchant or Acquirer would like protection from fraud-related chargeback liability under the Visa Rules, they can choose to submit a 3-D Secure authentication request to the Issuer who can then decide to perform SCA or apply an exemption.

**Table 4: Summary of EMV 3DS indicators and Field 34 indicators for the SCP exemption and associated Fraud Liability**

Exemption	Acquirer or Issuer applied	Authentication		Authorization	Fraud liability under Visa Rules <sup>12</sup>
		Merchant populated Exemption indicator in EMV 3DS Yes or No	ECI Value	Acquirer populated exemption indicator in authorization F34 Yes or No	
Secure Corporate Payment <sup>13</sup>	Submitted for authentication via 3DS prior to authorization				
	Issuer	Yes	7	Yes	Acquirer
	Issuer	No	5	No	Issuer
	Submitted straight to authorization				
	Issuer	N/A	7	Yes	Acquirer
	Issuer	N/A	7	No <sup>14</sup> Error! Bookmark not defined.	Acquirer

<sup>12</sup> Regulatory liability may differ

<sup>13</sup> This exemption can only be applied by the Issuer – but the indicator can be set by the Acquirer to indicate this exemption may apply

<sup>14</sup> It is not recommended (yet allowed) for an acquirer to submit this type of transaction without a value in Field It is best practice for the Acquirer to populate an exemption indicator or other informational indicator (Visa Delegated Authentication or Resilience indicator) in F34 when no authentication data is sent to the issuer