PSD2 SCA Commercial Cards Guide

March 2021

Version 1.1
05 March 2021

Contents

Important Information

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, 3-D Secure 2.0 and 3DS 2.0: When in this document we refer to 3-D Secure 2.0 or EMV 3DS this is a generic reference to the second generation of 3-D Secure and does not reference a specific version of the EMVCo specification. Version 2.1 of the specification is referred to as EMV 3DS 2.1 and version 2.2 is referred to as EMV 3DS 2.2

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 (subject to compliance with phased implementation plans).

Commercial cards are within the scope of the requirement to apply SCA, however some types of Commercial Card are not issued to individual cardholders and some transactions made using Commercial Cards are initiated using systems and processes that mean that where there is a cardholder, that cardholder may not be available to authenticate the transaction. There is therefore a risk that certain Commercial Card transactions could be declined due to it not being possible to apply SCA.

The PSD2 SCA Regulatory Technical Standards (RTS) includes the secure corporate processes and protocols exemption, referred to in this guide as the secure corporate payments (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. For more information, please refer to the *PSD2 SCA Secure Corporate Payment Exemption Implementation Guide*. Issuers of Commercial Cards are strongly encouraged to support and apply the exemption to qualifying transactions to minimise the risk of transaction declines where SCA cannot be applied.

Other than the ability to apply the SCP exemption to qualifying transactions, the requirements for the application of SCA to Commercial Cards, including out of scope transactions and other exemptions, are the same as for cards issued to consumers. More information on this can be found in *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

This guide aims to provide 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.

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

2. Commercial cards in the context of PSD2 SCA

2.1 Visa definition of Commercial Cards

Visa defines Commercial Cards as cards that may only be issued to provide a means of payment for business related goods and services and associated with an issuing BIN, account range or an account designated as one of the following type: Visa Corporate Card, Visa Business Card, or Visa Purchasing Card. The PSD2 SCA regulation impacts all Commercial Card types, as follows:

- **Physical Cards:** These are physical credit or debit cards issued to an individual named cardholder for business expenditure. These cards are sometimes referred to as "walking plastic".
- **Central Travel Account (CTA) and Lodge Accounts:** A card account that is issued to a corporate customer (a company or organization), not an individual, and is typically held by an agent, such as a Travel Management Company (TMC), approved by the corporate customer to make authorised travel purchases or bookings on behalf of the corporate customer. No physical card is issued. 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 (although the booking may be made via intermediaries acting on behalf of the customer and/or supplier). Alternatively, the transaction may be between the corporate customer and the TMC. This will be the case where the payment is for the TMC's fees and charges, and/or where the TMC is recharging for services they have already paid the supplier for through another payment method.
- **Accounts that are "lodged" or embedded with B2B merchants:** A card account that is issued to a corporate customer, not an individual, and is lodged/embedded directly with a merchant by the corporate customer (although the order may be made via intermediaries acting on behalf of the customer and/or supplier).It is used by the merchant to charge for agreed goods and services ordered by the customer. No physical card is issued.
- **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. 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. 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:

- Travel agencies settling booking payments with hotels,
- 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
- Corporates paying a supplier for an invoiced amount for goods/services rendered.

2.2 The application of SCA to transactions using Commercial Cards

PSD2 requires that SCA is applied to all electronic payments - including proximity and remote payments - within the EEA and the UK. This requirement applies to all transactions undertaken using Commercial Card products unless:

- The transaction is out of scope of the regulation; or
- The transaction qualifies for one of the exemptions defined in the PSD2 SCA RTS.

Notably, for e-commerce, SCA must be applied to transactions made using physical Commercial Cards used outside of a secure corporate environment, for example for direct bookings or purchases using a merchant's public website, unless the transaction qualifies for an exemption other than the SCP exemption or is out of scope.

The key consideration from the perspective of payments made using Commercial Cards is that a named cardholder must be available to complete the authentication process when SCA is required for a transaction. This may be not be possible for some Commercial Card transactions for one or more of the following reasons:

- Some types of cards, notably CTAs, lodged accounts and virtual cards, are not issued to an individual named card holder who could authenticate
- In some use cases, the processes used to initiate transactions are such that the cardholder will not be available to authenticate when the transaction is initiated, for example the booking of travel by a Travel Management Company (TMC) on behalf of a cardholder
- Some practices adopted within corporate customers mean payments may be made by a person who is not the named cardholder of the card being used, and the named cardholder may not be available to authenticate

If SCA is not applied when required, and unless the transaction is out of scope or qualifies for the SCP exemption or another exemption, the Issuer may need to decline the transaction.

2.3 Out of Scope Transactions

The following transaction types are out of scope of SCA:

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

For more information on the definition, identification and processing of out of scope transactions please refer to *PSD2 SCA Remote Electronic Transactions Implementation Guide*

2.4 Exemptions & Delegated Authentication

2.4.1 Exemptions

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

The following are some of the more important exemptions which may be applicable to transactions made using Commercial Cards, as well as for cards issued to consumers:

- The Transaction Risk Analysis (TRA) exemption
- The trusted beneficiaries exemption
- The low value transaction exemption

In addition, transactions made using commercial cards may qualify for the SCP exemption. To support the application of this exemption, Visa has introduced an SCP exemption indicator in Field 34 of the authorization message and an SCP indicator in EMV 3DS. These indicators allow transactions originating from secure corporate purchasing systems or travel management systems to be flagged to Issuers via either the direct to authorization or 3DS flows and enable a transaction to be processed without authentication, so long as the Issuer supports the exemption, and the requirements of the SCP exemption are met. Without this indicator present in a transaction made with a physical commercial card, the exemption cannot be used as Issuers will not know the exemption may apply.

More detailed guidance on the application of exemptions is given in the *PSD2 SCA Secure Corporate Payments Exemption Implementation Guide* and the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

2.4.2 Delegated authentication

The EBA has confirmed that PSD2 allows PSPs to outsource authentication to an entity to conduct SCA on their behalf. Visa has put in place a Delegated Authentication Program that provides a contractual framework to enable Issuers and Acquirers to delegate authentication to qualified delegates (such as merchants). Delegated authentication may be applied to transactions made using commercial cards subject to Issuer, Acquirer and delegate participation in the program and requirements of the program being met.

More detailed guidance on the application of delegated authentication is given in *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

3. Facilitating the application of SCA & exemptions for commercial card payments

Issuers of commercial cards should take the following steps to ensure that:

- Customer friction and abandonment are minimised
- The application of exemptions is optimised to minimise the need for SCA challenges and to ensure that challenges are not applied when it is not possible to complete them
- SCA can be applied when required and that the challenge process offers minimal friction
- Transactions do not get unnecessarily declined

3.1 Enroll all Commercial Cards in 3DS

3-D Secure (3DS) is the main mechanism used for authenticating payment transactions and managing the use of exemptions under PSD2 SCA.

Issuers should enroll all commercial cards in EMV 3DS, including CTAs, lodged and virtual cards to ensure that:

- SCA can be applied where it is required, for example to transactions using a physical commercial card for purchases made via a public website
- Merchants are able to correctly submit transactions made with all commercial card types and do not reject transactions as a result of the PAN not being known to EMV 3DS

Issuers should note this is essential as a merchant is unable to identify the type of Commercial Card being used from the PAN provided to them. When the merchant receives the PAN it is recommended Visa guidance that they first check to see if the PAN is known to EMV 3DS[1] before deciding how to proceed with the transaction. If a PAN is not known to EMV 3DS, the merchant may not know how to proceed with the transaction and the transaction may therefore be stopped or lost. The merchant could alternatively/or subsequently submit the transaction straight to authorization, in which case the Issuer can recognize that it is a CTA, lodged account or virtual card and apply the SCP exemption.

Enrolling all card ranges in EMV 3DS, including virtual cards, CTA and lodged accounts, enables the merchant to also submit the transaction via EMV 3DS and receive a correct response to an Authentication Request (AReq). Where the PAN represents a virtual card, CTA or lodged account, the Issuer is then able to apply the SCP exemption via the EMV 3DS flow, if the merchant/Acquirer has submitted the transaction via EMV 3DS. Issuers of virtual cards, CTAs and lodged accounts should note that they will need an Access Control Server (ACS) in order to enroll all their commercial card PANs in EMV 3DS and to respond to the merchant authentication request. Whether the merchant specifically requests the SCP exemption or not as a part of the EMV 3DS authentication, the ACS should also be instructed to apply the SCP

[1] Merchants/3DS Server operators should be performing a (Preparation Request) PReq at a minimum daily (at most once an hour) in order to maintain an up to date listing of BINs and account ranges.

exemption on virtual card, CTA and lodged BIN/account ranges if the Issuer approves the transaction and supports this exemption.

3.1.1 SCP Exemption and the Visa Attempts Server

EMV 3DS transactions with the SCP exemption indicator set in EMV 3DS by the merchant/Acquirer 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)
- ECI 07 (Acquirer liability)

Merchants are advised upon receiving such a response that 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.

3.2 Ensure the Secure Corporate Payments Exemption can be applied where possible

Since it is not possible to apply SCA to many transactions undertaken with Commercial Cards, it is critical that the SCP exemption is applied wherever possible. However, the conditions governing the use of the exemption are restrictive and there is uncertainty over interpretation of the regulation with regard to the exemption by NCAs. Individual NCAs may govern the application of the exemption in different ways. Furthermore, there are complex considerations to take into account in terms of practical application of the exemption. More detailed guidance on the application of the exemption is given in the *PSD2 SCA Secure Corporate Payments Exemption Implementation Guide*. Key steps that Issuers should take are summarised below.

3.2.1 Liaise with relevant NCAs

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

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

For more detailed guidance please refer to the *PSD2 SCA Secure Corporate Payments Exemption Implementation Guide*

3.2.2 Allocate dedicated account ranges within Commercial Card BINs for virtual card, Central Travel Account & lodged account issuance

Merchants may not be able to recognise that a transaction is completed using virtual cards, CTAs or lodged accounts and consequently may not know to apply the SCP indicator in EMV 3DS or in authorization. Issuers must therefore ensure these transactions are identifiable by their BIN or location within the BIN to apply the exemption themselves both at 3DS level and at authorization even when not requested by the merchant/Acquirer with the use of the indicator. Issuers should ensure dedicated account ranges within Commercial Card issuing BINs are used for these products as required by Visa rules (ID# 0026396).

3.2.3 Multinational issuing

Issuers of commercial products may issue cards, including virtual cards, CTA and lodged accounts in one country to corporate payers and/or employees of their corporate customer based in a different EEA country or in the UK using Visa's Multinational Program Issuance rules. Where those card products will be used within a secure corporate process and Issuers intend to use the SCP exemption as recommended, Issuers should ensure they have liaised with the relevant NCA to meet the local application of the SCA regulation for this exemption.

The regulation places the responsibility on the individual NCA to define the processes and criteria for registering and assessing secure processes and protocols. These may vary between countries and Issuers need to be aware of these differing requirements for each relevant NCA.

3.3 Support & apply other exemptions when the SCP exemption cannot be applied

Issuers should take steps to maximise the application of other qualifying exemptions, where the SCP exemption cannot be applied. Issuers should

- Ensure that the TRA exemption is applied where transactions qualify
- Consider supporting the trusted beneficiaries exemption for Commercial Cards and offering this option to corporate customers whose transactions do not qualify for the SCP exemption. This may for example, be appropriate where a corporate customer's bookings or purchases are for services or products provided by a known list of preferred merchants that can be added to cardholder's Trusted List. However, 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

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

For more information on the application of other exemptions please refer to the *PSD2 SCA Optimisation Best Practice Guide* and the *PSD2 SCA for Remote Electronic Transactions Implementation Guide*.

3.4 Select appropriate challenge methods for applying SCA to transactions undertaken using physical Commercial Cards

Issuers should consider adopting SCA challenge methods for physical Commercial Cards that minimise checkout friction while being appropriate to the needs and card usage patterns of Commercial Cardholders.

The currently recommended SCA challenge solutions for all card transactions are either Out of Band (OOB) app plus biometric or SMS OTP plus behavioural biometric. Issuers of Commercial Cards should take account of considerations including:

- Individual commercial credit cardholders may not have an Issuer provided online banking app in the way that they would for a consumer account, therefore a dedicated authenticator app may be required if an out of band app is one of the selected challenge solutions
- Some cardholders may make irregular Commercial Card ecommerce transactions. This may make it harder for customers to remember knowledge factors and provide

fewer interactions for building behavioral biometric profiles. Use of a native device operating system biometric to provide an inherence factor could overcome these challenges but will require cardholder education to ensure that an authentication app is installed, kept updated and not deleted.

- Some SCA methods may not work in some corporate environments. For example, some companies may restrict the use of company issued mobile phones in some environments, and/or mobile coverage may be poor or blocked. In these cases, it may be necessary to use methods that do not rely on mobile coverage or advise customers that their employees may be unable to complete transactions made in restricted environments.

Additional guidance on selection of challenge methods is included in the *PSD2 SCA Challenge Design Best Practice Guide*.

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

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

3.5 Provide guidance to corporate customers to minimise the risk of transaction declines & maximise the ability to take advantage of exemptions

Issuers should ensure they communicate the need to authenticate with their corporate customers and that corporate customers understand the implications including the following:

3.5.1 Physical Commercial Cards must not be shared

In some businesses it has become practice for physical Commercial Cards issued to specific individuals to be used by colleagues to make corporate purchases. For example, a single card may be used by multiple employees in a purchasing department or an executive's Commercial Card may be used by their personal assistant to book travel.

These practices are incompatible with the application of SCA and Issuers should advise their corporate customers that individual cards should be issued to each employee that needs to use a card to make purchases. Where necessary, corporate customers should modify administrative processes to ensure that purchases are correctly allocated and authorized in expense management systems.

3.5.2 Employees using Commercial Cards must have suitable devices to apply SCA

Where Issuers are using challenge methods that require the use of a mobile device to authenticate, for example an OOB app plus a biometric or SMS OTP, they should advise their customers on steps that need to be taken to ensure that such devices are available to employees and able to communicate. These may include:

- Ensuring that any security restrictions applied to company provided and managed devices allow the Issuer's authentication app to be installed and to operate
- Ensuring that device phone numbers are registered with the Issuer and able to receive authentication messages

- Ensuring that employees needing to authenticate are advised that they may need to install and register an app and the device biometric and that the number of this device will need to be the one registered with the Commercial Card Issuer
- Advising employees that are not issued with a company provided device that they will need to use their personal device and addressing any security or privacy concerns this may raise
- Ensuring that employees are briefed on why and how they will need to authenticate transactions made using the Commercial Card

3.5.3 Review purchasing processes to take account of SCA & maximise the ability to take advantage of exemptions

Issuers need to ensure that their Commercial Card product 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. This may include:

- The ways in which the Issuer supports the SCP exemption. For example, whether it supports the use of the SCP indicator by merchants and Acquirers, and whether it recognises transactions made using virtual cards and CTAs/lodged cards, and is able to apply the exemption to transactions made using those products
- Changes to business practices and purchasing processes that the customer and its purchasing partners (for example TMCs) may need to make to prevent transactions failing and to facilitate the application of the SCP, and other exemptions
- The customer's choice of Commercial Card products in order to facilitate the application of the SCP exemption, for example considering the use of CTAs or virtual cards for travel related transactions

4. 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 https://eba.europa.eu/single-rule-book-qa/qna/view/publicId
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 Secure Corporate Payments Exemption Implementation Guide	Version 1.1 March 2021	Contains more detailed guidance on the application of the secure corporate payments (SCP) exemption.
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: https://www.emvco.com/emv-technologies/3d-secure/

Glossary

Table 2: Glossary of terms

Term	Description
1-9	
3-D Secure (3DS) 2.0	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. The current version of 3DS is referred to as EMV 3DS. Two versions 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. Visa owns 3DS 1.0.2 and licenses it to other payment providers. EMVCo owns EMV 3DS. Visa's offering of 3DS is called Visa Secure.
A	
Access Control Server (ACS)	A server hardware/software component that supports Visa's EMV 3DS Program and other functions. The ACS is operated by the Issuer or the Issuer's processor. In response to Visa Directory Server inquiries, the ACS verifies that the individual card account number is eligible for authentication, receives authentication requests from merchants, authenticates the customer, and provides digitally-signed authentication response messages (containing the authentication results and other Visa's EMV 3DS Program data) to the merchant.
Authentication	Authentication allows the Issuer to verify the identity of the cardholder or the validity of the use of the card, including the use of the cardholder's personalized security credentials and, where required, takes place before authorization, using the Issuer's selected authentication method, which in most cases will be 3-D Secure
Authorization	Authorization determines if a specific transaction request receives an approval or a decline from the issuing bank, or from VisaNet standing in on the issuing bank's behalf. Once a cardholder initiates a purchase, VisaNet informs the Issuer of

Term	Description
	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	
Commercial Card	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 product types: • Visa Corporate Card • Visa Business Card • Visa Purchasing Card These product types may be issued as physical cards, virtual cards, Central Travel Accounts or lodged accounts. Note: Central Travel Accounts and lodged accounts are also sometimes referred to as "Ghost Cards"
E	
Exemption	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: • Low value exemption • Recurring payment exemption • Trusted beneficiaries exemption • Secured corporate payment exemption • Transaction Risk Analysis
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.
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[2].

[2] 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

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).
R	
Regulatory Technical Standards (RTS)	An RTS is a standard that supplements an EU directive. An RTS is developed for the European Commission, in the case of PSD2 by the European Banking Authority (EBA) and is then adopted by the Commission by means of a delegated act. The PSD2 SCA RTS, (formally titled *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*) 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.
S	
Strong Customer Authentication (SCA)	SCA, as defined by PSD2 SCA RTS, requires (among other things) that the payer is authenticated by a PSP through independent factors from at least two of the categories of knowledge, possession and inherence.
T	
Transaction Risk Analysis (TRA) Exemption	Under the Transaction Risk Analysis (TRA) exemption, PSPs may bypass SCA for remote transactions provided risk analysis is applied and the PSP's fraud rates, and transaction amounts are under certain thresholds (Article 18 of the PSD2 SCA RTS). The formula to calculate the PSP's fraud rate for the application of the TRA exemption is total value of unauthorized and fraudulent remote card transactions divided by the total value of all remote card transactions.
Trusted Beneficiaries Exemption	An exemption defined in the PSD2 RTS that allows, subject to certain restrictions, that a payer may add a trusted merchant

Authentication (SCA). Merchants and PSPs should check with NCAs for enforcement timescales in their respective markets.

.

Term	Description
	to a list of trusted beneficiaries (Trusted List) held by their Issuer, completing an SCA challenge in the process. Sometimes referred to as "whitelisting".
V	
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 Consumer Authentication Service (VCAS)	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.