


SCA impacts the business travel market

Strong Customer Authentication (SCA) is a EEA & UK regulatory requirement¹ under PSD2 designed to make payments more secure. It means on occasion, cardholders will be required to authenticate themselves via the use of EMV 3DS technology², before completing checkout.



This presents a significant impact on Travel Management Companies (TMCs) and other companies using Corporate Booking Tools (CBTs)/ Online Booking Tools (OBTs) where the cardholder is not always available to authenticate, or there is not a cardholder associated with the card.

Introducing the Secure Corporate Payment (SCP) exemption

Not all transactions require SCA – in fact, several payment types are either out-of-scope or qualify for an exemption

The SCP exemption allows issuers to not apply SCA where a business payment is made with an eligible commercial card through:

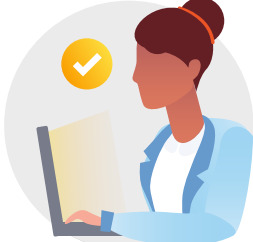
A dedicated secure corporate process that meets the security protocols set by the National Competent Authority (NCA) – which is generally the case for business travel and hospitality bookings made via a TMC or another company using a CBT/OBT.




Issuers need to have informed their NCA that they will use this exemption and assured them that the security measures provided are at least equivalent to those required within PSD2 – SCA will be required where the issuer does not support the SCP exemption.

How the process can qualify as 'secure' for the SCP exemption

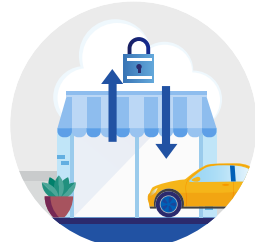
The process used by TMCs and CBTs must meet at least the following criteria for payments associated with their bookings




The booking process is only used for business related expenditure and by permitted users (corporate employees)




It must be protected by access controls with a level of security which meets PSD2 requirements



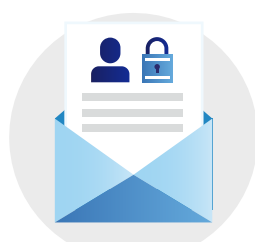
It is connected to merchants (directly or via intermediaries) that will process the payment using the SCP exemption via a secure electronic connection, e.g. secure API connectivity (not screen scraping).



The T&Cs of the purchase or booking are clearly displayed to the cardholder, including if transactions are to be later initiated by the merchant (MIT)



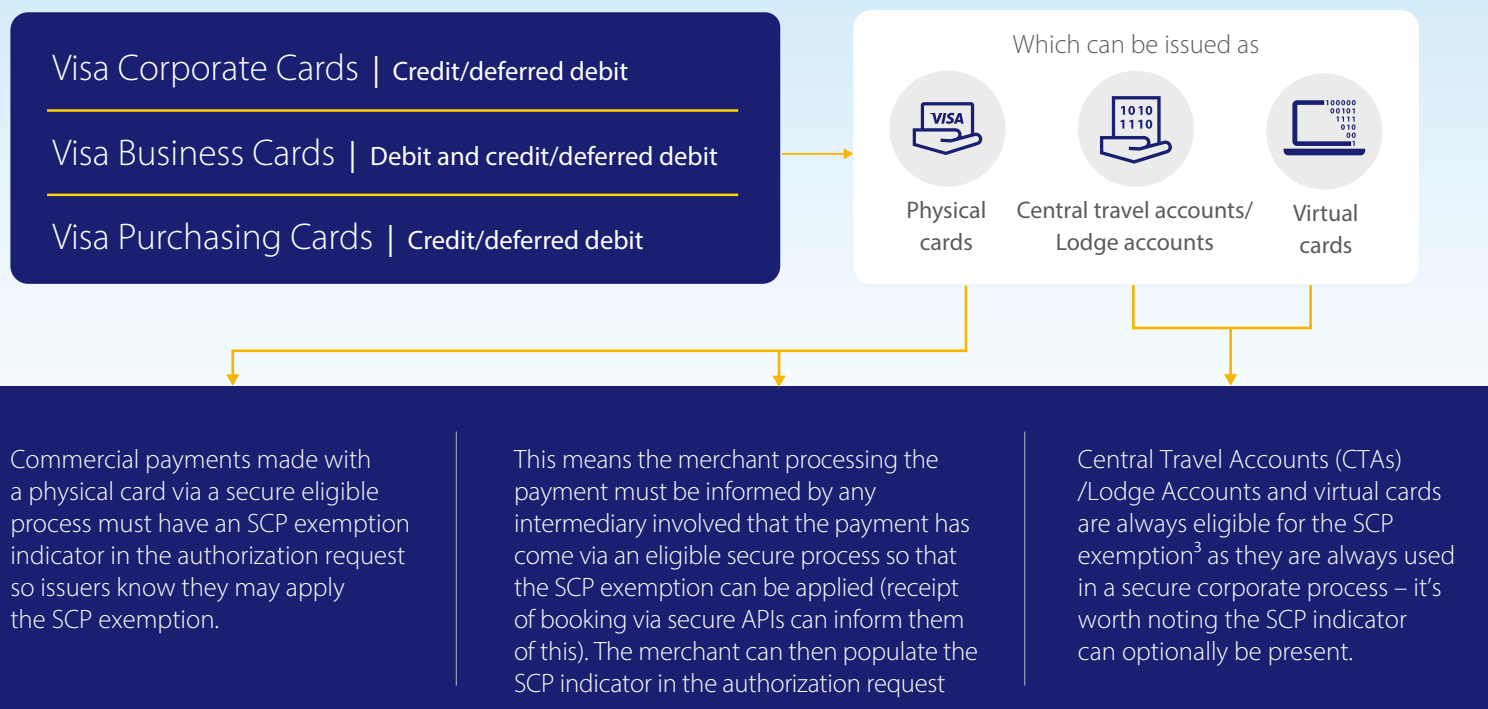
It meets Payment Card Industry Data Security Standard (PCI DSS) certification



It complies with General Data Protection Regulation (GDPR)

The SCP exemption in action for eligible commercial cards

If the TMC/CBT is certain that only eligible cards are used in their tool and the issuer supports the exemption, they can rely on the SCP exemption and skip the authentication step, to avoid unnecessary friction and declines.



Critically, when authentication is skipped and as a result the issuer declines the transaction, the merchant may not have a way to recontact the cardholder to handle authentication

If card eligibility for the SCP exemption is uncertain, TMCs/CBTs/OBTs are strongly advised to have a 3DS provider.

This means merchants can route the transaction via EMV 3DS 2.2 first in conjunction with the SCP exemption indicator, so that the issuer may either:



Confirm support for the exemption



Authenticate the transaction per SCA

To learn more about SCA and the SCP exemption TMCs/CBTs/OBTs should;

- Speak to their corporate customer to identify whether their issuer supports the SCP exemption
- Get in touch with their PSP or Acquirer to see how they can help
- Review the PSD2 SCA Secure Corporate Payment Exemption Guide
- Or alternatively, reach out to a Visa representative

¹ This is enforced in the EEA since January 2021 whilst implementation has began gradually in the UK since 1 June 2021 for full enforcement by 14th March 2022

² Get in touch with your payment service provider (PSP)/acquirer to learn more about EMV 3DS.

³ Subject to regulatory approval.