SCA impacts business payments made with commercial cards

Strong Customer Authentication (SCA) is a EEA & UK regulatory requirement[1] 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 technology[2], before completing checkout.

This presents a significant impact for Business to Business (B2B) purchases 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 means that issuers do not have to apply SCA where a 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)

Issuers need to inform their NCA that they will support the exemption and assure 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

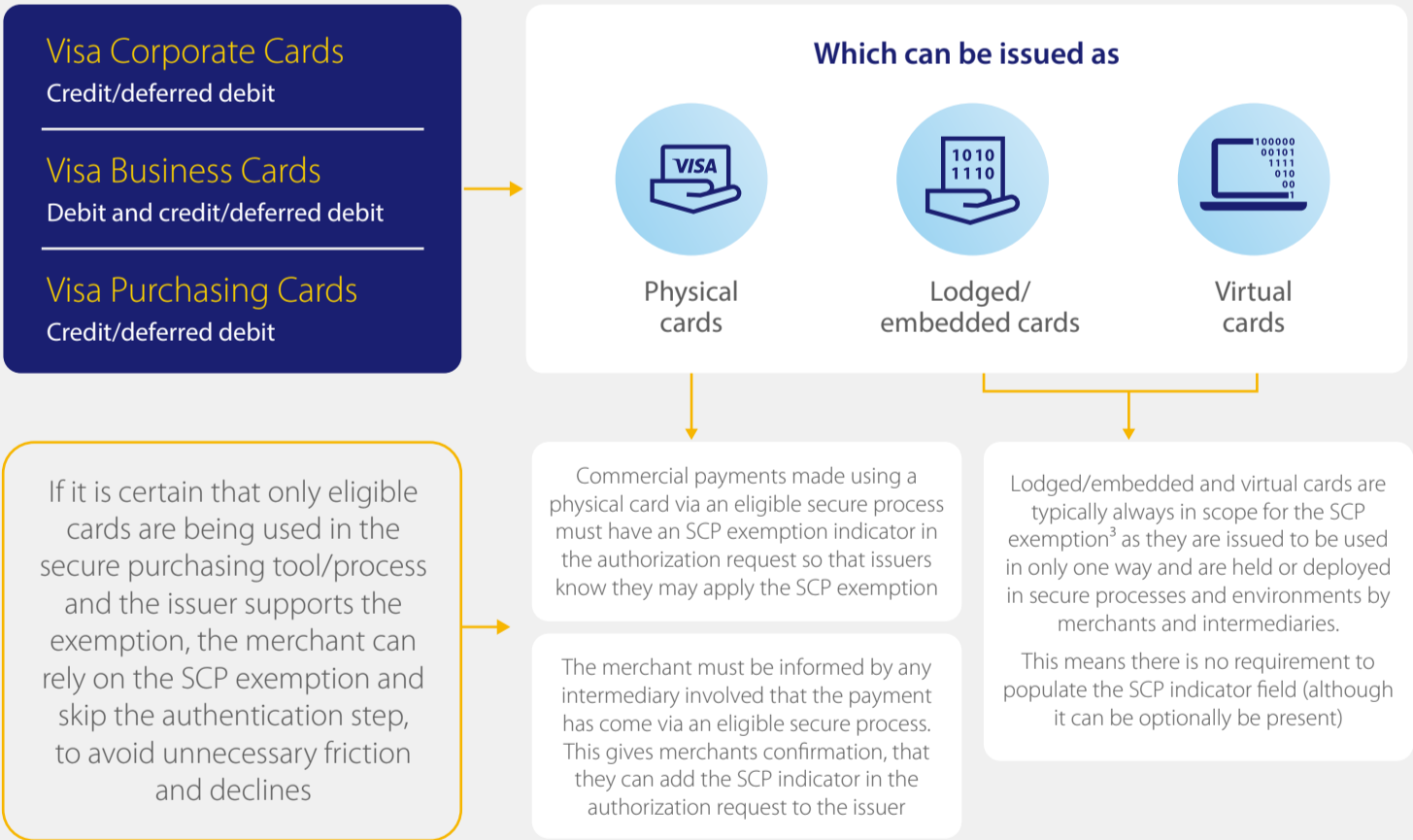# How the process can qualify as secure for the SCP exemption

The process used must meet at least the following criteria for associated payments:

- ✓ The process is only used for business related expenditure and by permitted users (corporate employees)
- ✓ It is protected by access controls with a level of security which meets PSD2 requirements
- ✓ It is connected to merchants that will process the payment using the SCP exemption via a secure electronic connection, e.g. secure API connectivity (not screen scraping)
- ✓ 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 commercial B2B scenarios

Eligible commercial cards used for business-related purchases can be issued in one of three ways:

Visa Corporate Cards
Credit/deferred debit

Visa Business Cards
Debit and credit/deferred debit

Visa Purchasing Cards
Credit/deferred debit

Which can be issued as

VISA	1010 1110	100000 00101 1111 010 00
Physical cards	Lodged/ embedded cards	Virtual cards

If it is certain that only eligible cards are being used in the secure purchasing tool/process and the issuer supports the exemption, the merchant can rely on the SCP exemption and skip the authentication step, to avoid unnecessary friction and declines

Commercial payments made using a physical card via an eligible secure process must have an SCP exemption indicator in the authorization request so that issuers know they may apply the SCP exemption

The merchant must be informed by any intermediary involved that the payment has come via an eligible secure process. This gives merchants confirmation, that they can add the SCP indicator in the authorization request to the issuer

Lodged/embedded and virtual cards are typically always in scope for the SCP exemption[3] as they are issued to be used in only one way and are held or deployed in secure processes and environments by merchants and intermediaries.

This means there is no requirement to populate the SCP indicator field (although it can be optionally be present)

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, the merchant is 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