PSD2 SCA Optimisation Best Practice Guide

July 2020

Version 1.0
15 July 2020

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, and Merchants 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, 3DS 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

Our goal is minimising friction while managing risk

PSD2 requires that Strong Customer Authentication (SCA) is applied to electronic payments within the European Economic Area (EEA) and the UK unless an exemption applies, or the payment falls into one of the out of scope categories.

There are a number of steps that merchants and payment service providers (PSPs) can take to minimise any friction experienced by customers making remote electronic payments, while maintaining compliance with the PSD2 SCA regulation. These include:

- Supporting the latest version of 3-D Secure, EMV 3DS 2.2
- Recognising and flagging out of scope transactions
- Optimising the application of exemptions to minimise the need for SCA challenges
- Optimising the experience of completing an SCA challenge when required.

Reducing customer friction is essential to optimising customer experience and minimising transaction abandonment.

The steps that merchants and PSPs should take to minimising friction can be grouped into two clear stages:

- Stage 1: Minimising the need for SCA challenges
- Stage 2: Creating a challenge process offering minimal friction when SCA challenges are required

The key steps in each stage are summarised overleaf.

This guide provides merchants, Acquirers and Issuers with guidance on Stage 1, minimising the number of transactions that will require Issuers to apply SCA challenges. See the *PSD2 SCA Challenge Design Best Practice Guide* for guidance on Stage 2, minimising friction when SCA challenges are required.

Please note that this is guide contains best practice guidance that aims to highlight the steps that merchants, gateways, Acquirers and Issuers can take to help to minimise friction and optimise the application of exemptions. For example, merchants should maintain low fraud rates to increase the likelihood that PSPs will apply exemptions. As such it provides a holistic view that recognises that all players have a part to play, although it should be noted that from a regulatory point of view, exemptions can only be applied by regulated PSPs.

Stage 1: Minimising the need for SCA challenges

	Merchant, Gateway & Acquirer	Issuer
STEP 1: Minimise fraud count	Maximise the option to apply exemptions by minimising mis-reported/friendly fraud through preventing/resolving disputed transactions	
STEP 2: Identify Out of Scope	Identify & correctly flag out of scope transactions	Recognise out of scope transactions & do not challenge them
STEP 3: Optimise risk management	Apply risk screening to best route transactions	Apply Risk Based Analysis to all transactions
STEP 4: Use 3-D Secure	Support EMV 3DS 2.2 or above to ensure exemptions are applied optimally	
STEP 5: Optimise for exemptions	Take full advantage of qualifying exemptions	Apply Issuer exemptions

Stage 2: Minimising friction when SCA is required

	Merchant, Gateway & Acquirer	Issuer
STEP 1: Optimise your SCA challenge strategy	Take full advantage of 3DS challenge window integration	Implement an holistic approach to serving low friction challenges
STEP 2: Maximise use of Biometrics	Pass all required 3DS data, ensuring it is correctly formatted, consistent & of high quality	Maximise the use of biometric & behavioural biometrics elements
STEP 3: Optimise onboarding & challenge UX	Fully utilise the UX integration & branding capabilities offered by 3DS	Simplify onboarding & challenge flows & ensure the UI is clear
STEP 4: Mitigate potential problems	Anticipate and mitigate potential user problems associated with challenge flows & provide effective customer communication & support	

All parties in the e-commerce and payments ecosystem have a role to play in minimising friction

All parties in the payments and e-commerce ecosystem including all merchants, gateways, 3-D Secure vendors, Acquirers and Issuers play a part in the application of SCA and all need to take steps to manage risk and ensure SCA challenges are only applied when required:

All parties have a part to play in reducing friction:

Larger Merchants

- Ensure e-commerce sites & apps support EMV 3DS 2.2 & pass required 3DS data
- Minimise disputes with use of pre-dispute tools
- Correctly flag out of scope transactions
- Deploy transaction risk screening
- Make full use of the acquirer TRA exemption
- Consider delegated authentication and usage of the trusted beneficiaries exemption

Smaller Merchants

- Ensure e-commerce sites & apps support EMV 3DS 2.2 and pass required 3DS data
- Correctly flag out of scope transactions
- Check whether payment providers can help with dispute prevention, transaction risk screening and PSD2 optimisation

Gateways, Acquirers & 3DS Server Vendors

- Educate & support merchants in adopting EMV 3DS 2.2
- Support use of pre-dispute tools
- Support merchants in applying the TRA exemption
- Ensure merchants can correctly flag out of scope transactions
- Optimise use of exemptions & challenge UX in hosted checkouts

VISA

- Develops and maintains EMV 3DS and Visa Attempts Server for Visa transactions
- Routes authentication requests via Directory Server
- Provides authorization message flags, tools & services to reduce friction
- Monitors performance to ensure the ecosystem delivers best in class experience to consumers while managing risk

Issuers

- Apply Risk Based Authentication to all transactions
- Do not challenge or decline unnecessarily
- Maximise the use of allowable exemptions
- Adopt SCA solutions that minimise friction

ACSs

- Fully use available data in RBA risk models
- Migrate from rules-based to AI based RBA
- Offer Issuers low friction SCA solutions
- Integrate with third party low friction SCA solutions
- Support 3RI

Step 1: Minimise fraud count

Disputes are often marked as fraud even when they are raised only because customers have trouble recognizing transactions and not because the transaction was unauthorised. Visa analysis indicates that fraud is reported 90% of the time a dispute is submitted[1].

Such disputes can artificially and unnecessarily inflate fraud counts, limiting the ability of Acquirers and Issuers to apply the TRA exemption and potentially limiting the ability of individual merchants to be considered for the application of certain exemptions[2].

Visa's experience has shown that a significant proportion of both disputes and transactions unnecessarily categorised as fraudulent can be avoided if customers and Issuers can be provided with additional information, such as the item purchased, to help customers validate transactions before they formally ask for a transaction to be disputed.

In 2019, merchants using Verifi solutions saw pre-dispute deflection rates[3] of up to 42%

If merchants provide this information to Issuers it enables them to deal more effectively with customer queries, improving customer satisfaction and removing these transactions from the fraud count. This can potentially improve the risk score of every transaction a merchant processes, while increasing the ability of Acquirers and Issuers to apply the TRA exemption. Merchants can also benefit by reducing revenue losses from disputes, as well as increasing their ability to qualify for the application of key exemptions.

Verifi, a Visa company, offers a suite of related Pre-dispute Products to help both merchants and Issuers avoid and resolve such disputes.

[1] Source: Visa analysis from Visa Resolve Online statistics

[2] From a regulatory perspective the ability to apply the TRA exemption is dependent upon the fraud rate of the PSP applying the exemption. From a wider perspective, Acquirers are more likely to consider applying exemptions to transactions from low fraud rate merchants. In some specific cases, for example, the Visa Trusted Listing program which facilitates the application of the trusted beneficiaries exemption, merchants need to meet fraud rate targets to be enrolled and remain within the program.

[3] The deflection rate measures the percentage of pre-disputes that were resolved at the point of inquiry, and do not subsequently become a chargeback.

Verifi Pre-dispute Solutions

Verifi pre-dispute solutions provide an opportunity for merchants, Acquirers and Issuers to collaborate and share data to prevent and resolve disputes at the pre-dispute stage.

Verifi's Order Insight® (formerly Visa Merchant Purchase Inquiry) allows merchants to share order details with Issuers through the existing **Visa Resolve Online (VROL)** dispute process. Enhanced transaction data is provided by merchants to Issuers for review with cardholders at first inquiry.

Order Insight Digital (formerly Visa Cardholder Purchase Inquiry) enables cardholders to access the same enhanced transaction data through an Issuer's online banking portal or mobile app. Validating the sale with the cardholder can help prevent a dispute from being raised. Global Visa Issuers are required to receive transaction data in **VROL** from participating merchants before submitting a dispute.

Rapid Dispute Resolution (**RDR**) operates at the pre-dispute stage to resolve disputes before they escalate, as determined by seller-defined rules in the Verifi automated decisioning engine. Pre-disputes from other card brands can also be resolved through Verifi.

From July 2020, all Verifi services are available through **VROL** for Issuers, or through enrolment directly with Verifi for merchants. Interested parties should contact Verifi (info@verifi.com), or speak to their Visa representative. Small to medium Merchants should speak to their Acquirer about availability of these services.

Step 2: Identify and flag out of scope transactions

What are out of Scope transactions?

The PSD2 regulation identifies some transactions as being “out of scope” of SCA. SCA does not need to be applied to out of scope transactions. Visa estimates that approximately 46% of remote transactions are out of scope.[4]

Transaction types out of scope of SCA	
Merchant Initiated Transactions (MITs)	A transaction, or series of transactions, of fixed or variable amount and frequency, governed by an agreement between the cardholder and merchant that, once agreed, allows the merchant to initiate subsequent payments without any direct involvement of the cardholder. Examples of MITs include subscription type payments at fixed or variable intervals, installment payments, pre/balance payments, payments related to delayed or split shipments, payments related to booking reservations made via indirect channels, cancellation fees (No show), incremental authorization requests, delayed charges, and collection of payment of already delivered services (contactless transit only). **In most cases SCA is required if the agreement is set up through a remote electronic channel and MITs must be identified and flagged by merchants so their Acquirers can flag them to Visa using the Visa MIT Framework.**[5]
Mail Order/ Telephone Order (MOTO)	Payments made through Mail Order/Telephone Order (telephone includes Interactive Voice Response services). Note, “voice commerce” payments initiated through digital assistants or smart speakers are not classed as MOTO. **These transactions must be identified and flagged by merchants and Acquirers.**[6]
One-Leg-Out (OLO)	A transaction where either the Issuer or Acquirer is located outside the EEA or the UK is considered out of scope and not requiring SCA. However, SCA should still be applied on a “best efforts” basis. **These transactions are identifiable by the issuer BIN or the Acquirer location being from outside the EEA or the UK.** [6]

[4] For more detail on identifying out scope transactions please see section 3.2.8 of Visa *PSD2 SCA for Remote Electronic Transactions Implementation Guide V2.0*

[5] For more detail see section 3.10 of the Visa *PSD2 SCA for Remote Electronic Transactions Implementation Guide V2.0*

[6] For more detail see section 3.2.8 of the *Visa PSD2 SCA for Remote Electronic Transactions Implementation Guide V2.0* Merchants should also check how their Acquirers would like them to flag out of scope transactions as some use a proprietary standard for merchant flags and then convert the flags to the appropriate card scheme standard before submitting an authorization request.

Anonymous transactions	Transactions through anonymous payment instruments, for example anonymous prepaid cards. **These transactions cannot be recognised as such by a merchant so must be identified by Issuers checking the BIN.**[6]

Note: Visa also considers that SCA is not required to be performed by the cardholder for the following types of transactions:

- Original Credit Transactions (OCTs)[7] and refunds, as the customer is receiving rather than making a payment
- Some zero value authorization/account verification requests[8]

Visa tools for out of scope transactions

The Visa MIT Framework

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

Visa authorization message indicators

Specific field values in Visa authorization system messages are provided to allow merchants to identify a transaction type that an Issuer must recognise as out of scope and does not require the application of SCA.

Issuers have the choice to recognise MITs using the Visa MIT Framework or the MIT out of scope flag in Field 34 of the authorization request.

Merchants & Acquirers need to identify and flag Out of Scope transactions

If a payment transaction is out of scope of SCA, the merchant/Acquirer must submit an authorization request that includes the information the Issuer will need to process it without SCA. Transactions that are not correctly flagged in this way are at risk of being declined by Issuers.

[7] OCTs are "push" payments that allow a Visa cardholder to receive funds to their eligible Visa card account in near-real time. For more detail see section 3.2.8 of the *Visa PSD2 SCA Implementation Guide Version 2.0*.

[8] In some limited use cases described in section 4.6.4 of *PSD2 SCA for Remote Electronic Transactions Implementation Guide Version 2.0*, SCA may be required. Refer to this section for more details on account verifications.

What merchants should do

Merchants who process out of scope transactions need to ensure that they can identify these transactions and populate the appropriate authorization indicators, as defined by their Acquirer. Note it is important that merchants check how their payment gateway/Acquirer would like them to identify MITs and other out of out of scope transactions. Some payment gateways/Acquirers use a proprietary standard for merchant flags and then convert the flags to the appropriate card scheme standard before submitting an authorization request.

To identify MITs to be recognised as out of scope and processed without the need for SCA, a merchant or their gateway must store the transaction ID from the initial agreement set up transaction (or, in some cases, from a previous MIT) They must then provide it, along with the indicator identifying the type of MIT, in each MIT authorization request they subsequently submit to collect payments under the agreement.

Merchants should speak to their Acquirer or payment gateway as soon as possible to agree which, if any, types of out of scope transaction they are processing, how setting up an MIT agreement should be authenticated, how all out of scope transactions should be identified and flagged, and how initial or prior transaction IDs should be captured, stored and populated into authorization requests.

For more information on out of scope transactions, MITs and the MIT framework

See the *Visa PSD2 SCA for Remote Electronic Transactions Implementation Guide V2.0*. This guide includes much more detail in section 3.2.8 on the ways in which out of scope transactions are identified and flagged. Section 3.10 describes the eight different types of MIT defined under the MIT framework and Section 5 includes explanations as to how MITs should be treated in a number of common and complex payment scenarios.

Issuers should not decline or request authentication for transactions that are identified as out of scope of SCA

Issuers must be able to recognise every type of out of scope transaction and must not decline or request authentication for transactions that have been flagged as out of scope by the Acquirer[9]. They should also be able to identify transactions acquired outside the EEA and the UK and transactions made with anonymous cards. Note it is important that one-leg-out transactions are identified using the Acquiring Institution country and not the merchant country code.

Visa Rule:

An Issuer must not use an SCA decline code for transactions deemed out of scope from a regulatory perspective. Issuers may only use an SCA decline code for these transactions when they believe the transaction has been incorrectly flagged/is not permitted under regulation to be out of scope[9].

Similarly, Issuers should not decline or request authentication for OCTs or relevant zero value authorization/account verification requests.

[9] For more information please refer to Section 4.5 of *PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area Visa Supplemental Requirements*

Step 3: Optimise risk management

Visa recommends that merchants undertake risk screening on transactions before submitting them to authentication or authorization. Issuers are required to apply Risk Based Analysis (RBA) to all transactions.

Merchants should use Risk Based Analysis (RBA) to minimise fraud rates and optimise application of exemptions

Merchants should ensure that RBA is part of their fraud screening processes, included prior to authorization or authentication, improving security and also setting the foundation for their SCA strategies.

The benefits include:

- Merchants are likely to have the best understanding of their customers and the fraud risks associated with their businesses
- The analysis undertaken by merchants can be used to apply for the Acquirer TRA exemption[10] and to enable merchants to decide whether:
    - They would like an exemption applied or,
    - They should submit a transaction via 3DS for potential application of SCA
- Merchants can also use this analysis to develop and execute exemption strategies to minimise customer friction and fraud liability risk

At its simplest level, RBA is based upon rules set by or in conjunction with the merchant to assess the risk of a transaction based upon simple characteristics of the transaction. More sophisticated solutions increasingly use machine learning based risk models and multiple datapoints to provide a much more accurate assessment of risk and minimise both fraud and false positives.

The approach taken by merchants will depend upon their size, resources and the risk profile of their business.

- Smaller merchants may choose by default to submit all of their transactions via 3DS leaving the Issuer to risk assess them and decide which transactions qualify for exemptions. However, a merchant who applies no RBA or fraud screening risks a higher fraud rate, the application of fewer exemptions and higher customer friction. It is recommended that such merchants speak to their payment gateway, acquirer or 3DS server provider to check what risk analysis and screening services they are able to offer.

[10] Note: The Acquirer TRA exemption can only be used based on the acquirer's overall fraud rate not any merchant-specific rate

- Larger and enterprise merchants should look to adopt more proactive strategies using more sophisticated risk tools to minimise fraud rates and take advantage of the ability to apply Acquirer exemptions and send transactions direct to authorization to minimise the impact on customer experience and authentication costs.

Merchants must align with their gateway/Acquirer to ensure that their SCA exemption strategy is supported.

CyberSource Risk Management & Exemption Decision Tools

CyberSource, a Visa owned company, offers a full stack of payment and fraud solutions. The **CyberSource Decision Manager** risk management platform includes an SCA exemption optimisation layer. This enables merchants to make risk-based decisions based upon their business rules, and subsequently request an exemption, via authorization or 3DS, or submit the transaction via 3DS for authentication.

CyberSource Decision Manager offers the following benefits

- A rules engine combined with machine learning based risk models that can detect high risk transactions and identify which transactions are out of scope of SCA or could qualify for an SCA exemption based on risk
- The ability to process exempted transactions direct to authorization to reduce customer friction and authentication costs
- When combined with CyberSource 3DS solutions, Decision Manager will have the future capability to automatically resubmit transactions sent direct to authorization via 3DS when an Issuer requires authentication.

For further information on CyberSource Fraud and Payment Management Solutions, existing CyberSource customers should contact their CyberSource account manager. Other parties can learn more, and contact CyberSource by visiting cybersource.com.

Issuers should use Risk Based Analysis (RBA) to minimise fraud rates and optimise application of exemptions

Managing risk effectively will enable Issuers to maximise their ability to apply exemptions. Issuers should aim to implement risk strategies that balance the need to keep fraud low whilst at the same time avoiding the need to challenge every single transaction. In the case of the TRA exemption, keeping fraud rates within the reference fraud rate for the highest achievable transaction value band can be achieved by making full use of 3DS data.

Issuers should set strategies that clearly define the risk score thresholds that require the application of a 3DS challenge. These strategies should ensure that, unless SCA is required by the regulation:

- SCA is only applied when the risk score exceeds a set threshold
- Issuers do not apply SCA to transactions that qualify for an exemption where the risk score is low. Doing so will unnecessarily increase friction and transaction abandonment
- Risk scoring & challenge strategies are regularly reviewed against fraud and transaction abandonment data and adjusted as necessary to ensure the optimum balance is maintained
- Where and when possible, Issuers adopt risk engines that use machine learning as a more effective alternative to rules-based scoring.

Visa Rule:
Issuers are required to support RBA for EMV 3DS and must evaluate the risk level of each transaction using some form of risk-model, rules engine, or risk analysis, and then apply the required authentication procedure.

Visa tools for Risk Based Analysis (RBA)

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. The VCAS risk model is uniquely able to access the most comprehensive transaction data set drawn from across the Visa's global network and third-party sources. VCAS assesses the risk of a transaction in real-time using predictive risk analysis based on a number of enhanced inputs, including device and transaction information and behaviours. This network-wide level of intelligence gives Issuers the analysis required to decide if and when additional authentication is needed.

VCAS Score

VCAS Score is the risk assessment and transaction risk scoring engine behind VCAS. This offers a sophisticated AI based model utilising the most comprehensive transaction data available to Issuers who use the VCAS ACS.

The VCAS solution has been built in partnership with CardinalCommerce, an industry leader in digital payment authentication that is fully owned by Visa. For more information please see https://www.cardinalcommerce.com/products/visa-consumer-authentication-service.

Step 4: Use 3-D Secure

3-D Secure (3DS) is the leading industry standard solution being used across the card payments industry to apply SCA.

What is EMV 3DS 2.2 and why is it important?

The latest version of 3DS, EMV 3DS 2.2, provides critical new functionality that is fundamental to the optimisation of the application of PSD2 SCA and all permitted exemptions. All Issuers are mandated to support EMV 3DS 2.2 by September 14, 2020 and Acquirers are mandated to ensure their merchants are connected to vendors who support it by October 16 2020.

EMV 3DS 2.2 also provides new functionality required to authenticate some complex payment use cases and offers a better user experience than previous versions of 3DS. It supports purchases made through browsers, mobile apps and other devices.

EMV 3DS 2.2 critical new functionality

Exemptions: Indicators that enable merchants and Acquirers to take advantage of SCA exemptions (TRA, secure corporate payments & trusted beneficiaries)

SCA Delegation: The Visa Delegated Authentication program allows Issuers to delegate the performance of SCA to selected merchants or token requestors. Indicators enabling delegation are included in EMV 3DS 2.2

3RI - Allows SCA and exemptions to be applied in complex merchant use cases such as travel bookings or split shipments and for refreshed cryptograms to be issued once expired: a particular benefit for delayed shipments

Authenticating with mobile apps: Improved re-directs to apps or other external environments via the Out of Band (OOB) function

Biometrics: A more seamless transition to an app makes biometric authentication easier for consumers

What merchants should do

Merchants must support 3DS to facilitate the application of SCA which is required under PSD2 and Visa strongly encourages merchants and Acquirers to support EMV 3DS 2.2 as early as possible.

Merchants new to EMV 3DS should note that it is a different protocol to 3DS 1.0, and they will need a 3DS Server rather than an MPI to support it. Those who process transactions through a mobile app will need to integrate the 3DS SDK.

EMV 3DS data quality

EMV 3DS also requires that merchants submit additional transaction data[11] with the authentication request message. This data is used by Issuer's ACS providers to analyse the risk of the transaction and can reduce the number of transactions for which SCA is applied. It is critical that this data is correctly formatted, consistent and of high quality in order to avoid Issuers having to apply SCA just because they have insufficient data to risk assess a transaction. Merchants should pay particular attention to the Browser IP, Shipping Address Postal code, Billing Address Postal code, and Address match indicator as key fields. However, in general, the more quality data that the merchant is able to supply over time (regardless if it is optional or required), the more it can assist in the risk analysis of the transaction.[12] A further critical factor in the gathering of data is the use of the 3DS Method URL. If a 3DS Method URL is specified, then merchants should be using this for the appropriate flows.

All merchants should speak to their Acquirer, payment gateway and/or 3DS provider to plan their migration to EMV 3DS 2.2.

[11] Merchants should refer to the PSD2 SCA for Remote Electronic Transactions Implementation Guide for detailed information of 3DS data requirements

[12] Also see https://www.ukfinance.org.uk/system/files/Strong%20Customer%20Authentication%20-%20Communication%20on%20improving%20outcomes%20from%203DSecure%20–%20Data%20Consistency_1.pdf

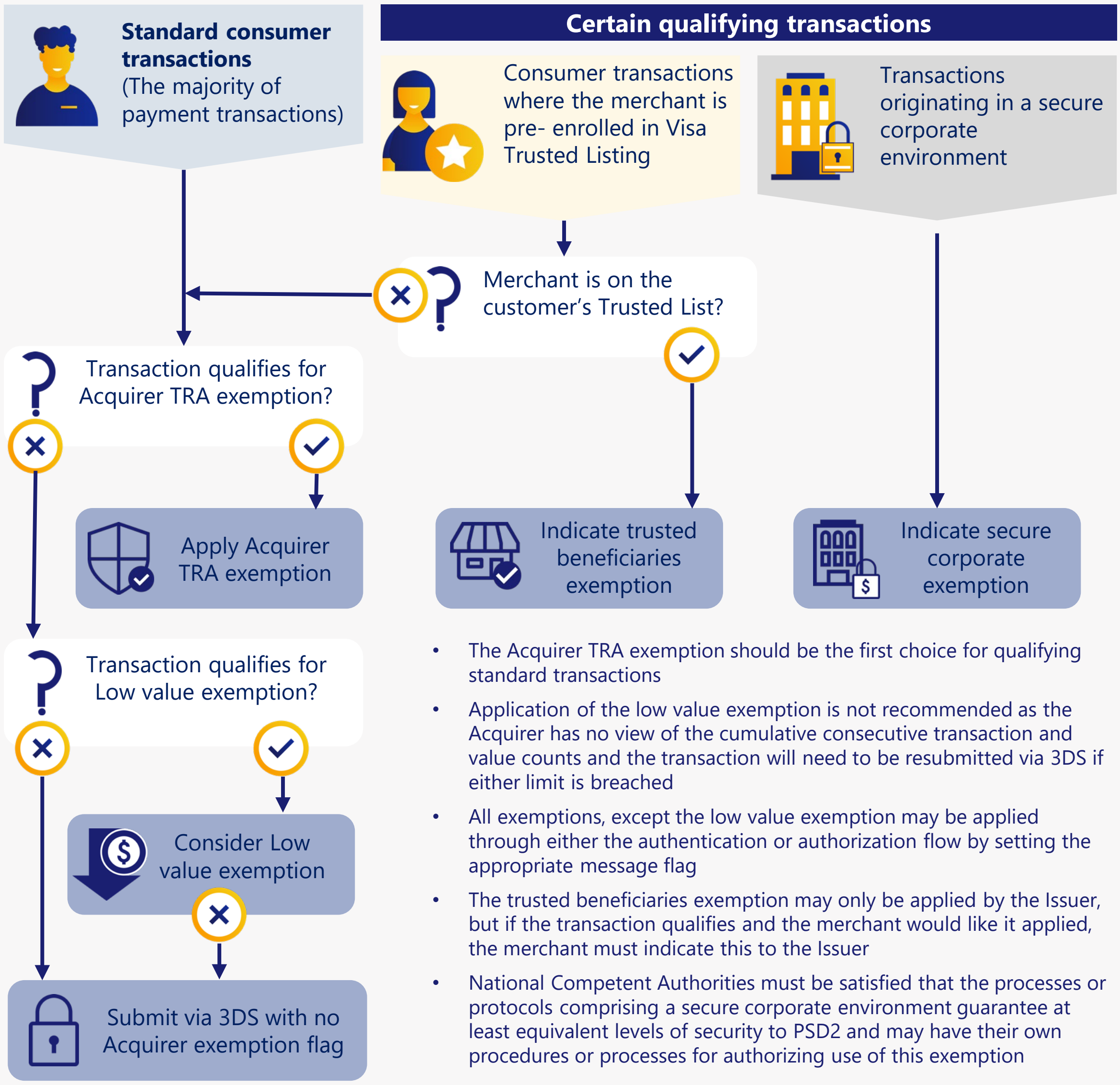
Step 5: Optimise for exemptions

Guidance for merchants and Acquirers on the application of exemptions

Which exemption should be applied first?

The following logic should help merchants and Acquirers to select which, if any, allowable exemption to apply or request[13].

Merchant/Acquirer choice of exemption depends on transaction type:



Standard consumer transactions (The majority of payment transactions)

Certain qualifying transactions

Consumer transactions where the merchant is pre- enrolled in Visa Trusted Listing

Transactions originating in a secure corporate environment

Merchant is on the customer's Trusted List?

Transaction qualifies for Acquirer TRA exemption?

Apply Acquirer TRA exemption

Indicate trusted beneficiaries exemption

Indicate secure corporate exemption

Transaction qualifies for Low value exemption?

Consider Low value exemption

Submit via 3DS with no Acquirer exemption flag

- The Acquirer TRA exemption should be the first choice for qualifying standard transactions
- Application of the low value exemption is not recommended as the Acquirer has no view of the cumulative consecutive transaction and value counts and the transaction will need to be resubmitted via 3DS if either limit is breached
- All exemptions, except the low value exemption may be applied through either the authentication or authorization flow by setting the appropriate message flag
- The trusted beneficiaries exemption may only be applied by the Issuer, but if the transaction qualifies and the merchant would like it applied, the merchant must indicate this to the Issuer
- National Competent Authorities must be satisfied that the processes or protocols comprising a secure corporate environment guarantee at least equivalent levels of security to PSD2 and may have their own procedures or processes for authorizing use of this exemption

[13] The regulation allows Acquirer application of the recurring transaction exemption however Visa does not support this exemption. Subscription type payments at fixed or regular intervals should, where appropriate, be processed as MITs (out of scope) in the Visa system.

Acquirers may, subject to transaction value and their fraud rate, apply either the TRA exemption or the low value transaction exemption. Issuers may apply any of the exemptions.

Merchants may indicate that they would like Issuers to apply the trusted beneficiaries exemption and may flag to Issuers that a transaction qualifies for the secure corporate payments exemption. The order in which exemptions should be applied or requested by merchants and Acquirers depends upon the transaction type and whether the transaction qualifies.

Merchants should note that only one exemption should be applied or indicated in a given transaction and that Issuers have the final say on whether an exemption can be applied and may choose to apply a challenge to a transaction flagged with an exemption indicator if they consider it to be high risk.

What is the TRA exemption?

The TRA exemption allows for certain remote transactions to be exempted from SCA, provided:

1. A robust risk analysis is performed, and
2. The fraud rate of the PSP applying the exemption is within specific thresholds.

Fraud thresholds PSPs must meet to apply the TRA exemption

Transaction value band	PSP fraud rate
≤€100	13 bps/0.13 %
€100≤€250	6 bps/0.06 %
€250≤€500	1 bps/0.01 %

A merchant can take more control of their customer experience by working with their Acquirer to apply the TRA exemption. Note that fraud liability is with the party that applies the exemption.

What merchants should do to take advantage of the Acquirer TRA exemption

Merchants who undertake sophisticated risk screening should work with their Acquirer to develop strategies for when to apply the Acquirer TRA exemption.

Merchants should also ensure that they understand their Acquirer's fraud rate and should consider changing Acquirers if they would benefit from exemption being applied to higher value transactions.

What Acquirers can do to apply the TRA exemption

Acquirers have the flexibility to only allow certain low risk merchants to benefit from the TRA exemption and may use this in order to minimise risk and fraud rates.

For more information on applying the TRA and other exemptions

See sections 2.2 and 4.5 of Visa *PSD2 SCA for Remote Electronic Transactions Implementation Guide V2.0*. This guide includes more detail on the application of the exemptions. You may also get more information from your Acquirer or payment gateway.

Deciding how to route qualifying transactions: via 3DS or straight to authorization

All exemptions, except the low value exemption may be applied through either the authentication or authorization flow by setting the appropriate message flag[14].

If a merchant sends a transaction for authentication without requesting application of the TRA exemption, the Issuer may still apply it, so long as the transaction qualifies taking account of the Issuer's fraud rate and risk analysis.

Merchants should generally submit transactions for authentication via 3DS if:

- They are not requesting application of the exemption and would like to benefit from liability protection
- They/their Acquirer are unable to undertake the level of risk screening required in order to apply the TRA exemption
- Their analysis indicates the transaction is high risk and/or there is a risk that the Issuer may assess the transaction as being high risk and requiring SCA. This can include, for example, transactions that may qualify for the trusted beneficiaries exemption but are considered by the merchant to be high risk and therefore should be authenticated
- It is possible that authorization will be delayed, and the cardholder will be unavailable to authenticate if the Issuer requests resubmission for authentication
- The merchant would like the customer to have the option to add them to their Trusted Beneficiaries list

Otherwise, submitting a transaction direct to authorization can have the benefit of reducing potential friction, allowing the merchant to retain control of the user experience, however, note that the Acquirer accepts liability for transactions submitted straight to authorization. Merchants should also note that the Issuer still has the final say and may require that a transaction is resubmitted via 3DS for authentication – a process which may add latency and potentially additional friction.

[14] Please note that the Acquirer low value exemption may only be applied via the authorization flow and that the secure corporate payments exemption indicator is supported in the authentication flow from July 2020.

Taking advantage of the trusted beneficiaries exemption

The trusted beneficiaries exemption allows for the cardholder to add a trusted merchant to a list of trusted beneficiaries held by their Issuer, completing an SCA challenge in the process. Further SCA application on subsequent transactions with the trusted merchant should generally not be required[15].

The PSD2 regulation does not define a transaction value limit for the application of the trusted beneficiaries exemption, so it can be applied to transactions of any value.

Conditions on the application of the trusted beneficiaries exemption

- Only Issuers can apply the trusted beneficiaries exemption and create/maintain lists of trusted beneficiaries on behalf of cardholders: Acquirers cannot apply this exemption
- Only customers can add or remove a merchant to/from a Trusted List (although a merchant may invite the customer to do so)
- Additions to, and amendment of, the Trusted List requires SCA

Visa Trusted Listing (VTL) – why merchants should enrol

Visa has developed a capability which provides Issuers with the ability to create and maintain their customer's list of trusted beneficiaries within the conditions set by the regulation. **Visa Trusted Listing** enables enrolled merchants to request participating Issuers present to a customer who has not yet added the merchant to their Trusted List, the trusted beneficiary enrolment option form:

- When a customer completes a transaction with them, or
- Outside of the purchase experience, for example when a customer is creating an account with the merchant/saving a card on file

In either case the customer must complete an SCA challenge to add the merchant to their Trusted List.

A merchant that is on a customer's Trusted List, can indicate that it would like an Issuer to apply the trusted beneficiaries exemption to a transaction by using the trusted beneficiaries exemption indicator in 3DS.

The customer can manage their Trusted List (by making additions, or by removing merchants) through an Issuer controlled experience. The merchant may provide the mechanism for a customer to trigger addition or removal, or see whether the merchant is on the customer's Trusted List, however the actual process of addition and removal must be undertaken through the Issuer.

[15] Note an Issuer can still request SCA or decline a transaction if it assesses that transaction to be high risk.

Merchants with high customer visit frequency and low fraud rates should consider benefiting from this exemption. Acquirers should also consider which of their merchants would benefit from this exemption and Visa's solution. Merchants interested in VTL should work with their Acquirer to enroll.

Applying the Secure Corporate Payments Exemption

The secure corporate payment exemption is an exemption that may be applicable for transactions that are initiated from within secure corporate environments where Issuers have demonstrated to the National Competent Authority that the processes and protocols used satisfy the requirements of the regulation. These could for example, and subject to the view of local regulators, include corporate purchasing or travel management systems. Most transactions initiated through a secure corporate process cannot be authenticated by a cardholder.

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 secure corporate exemption flag. This enables a transaction to be processed without authentication, so long as the Issuer supports the exemption.

Acquirers will be provided with requirements and guidance from Visa in summer 2020 as to the conditions governing the use of this flag, which can be used in 3DS requests or for transactions sent direct to authorization.

Guidance for Issuers on the application of exemptions

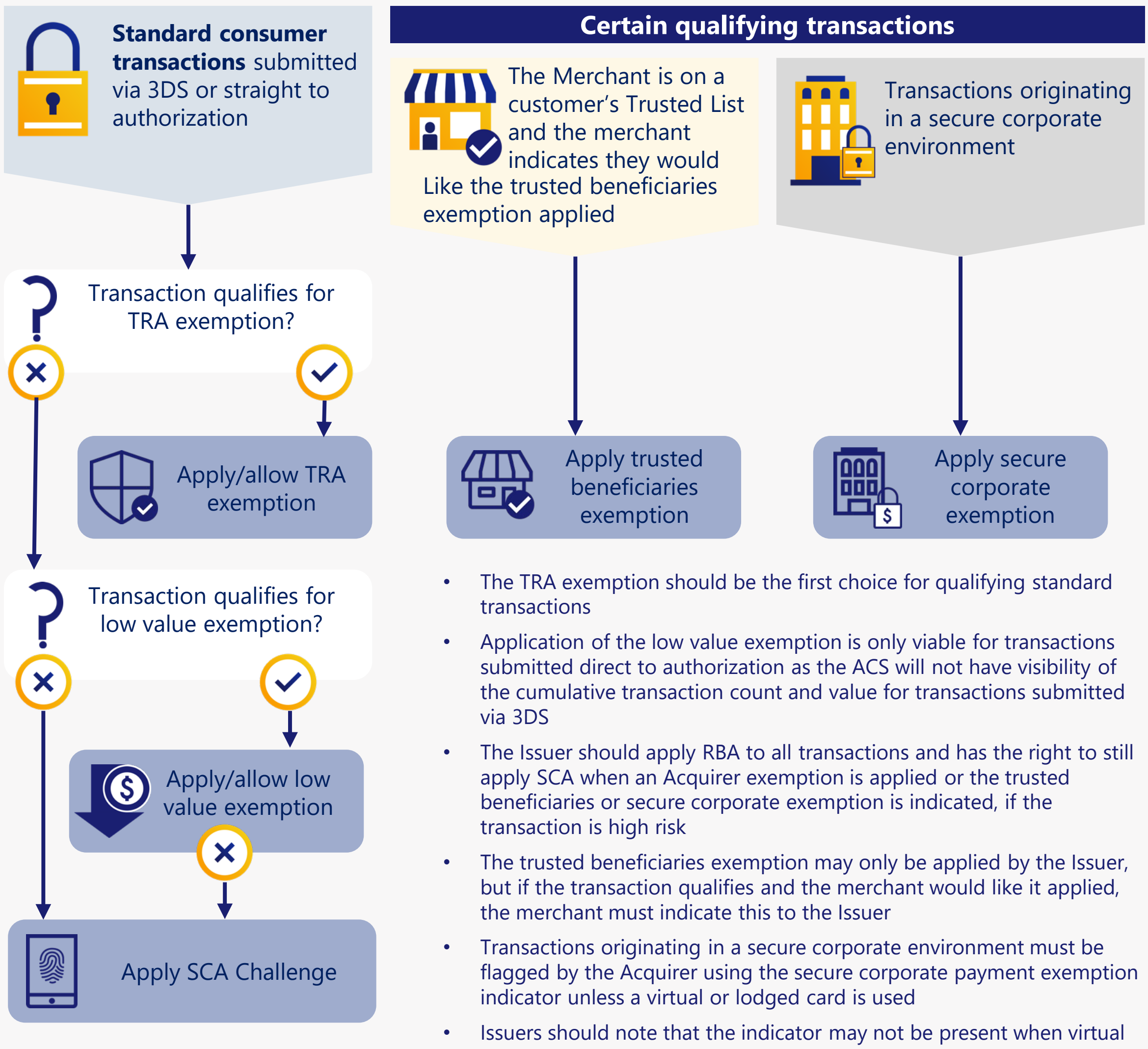
Apply exemptions to all qualifying transactions

Issuers should apply risk analysis to all transactions and generally:

- When transactions are submitted by Acquirers with an exemption flag (via 3DS or direct to authorization), allow the exemption unless analysis indicates the risk is high
- When transactions are submitted by Acquirers via 3DS without an exemption flag, apply exemptions to all transactions that qualify

The most appropriate exemption will depend upon the transaction type and the qualifying criteria:

Issuer choice of exemption depends on transaction type:



Standard consumer transactions submitted via 3DS or straight to authorization

Certain qualifying transactions

The Merchant is on a customer's Trusted List and the merchant indicates they would Like the trusted beneficiaries exemption applied

Transactions originating in a secure corporate environment

Transaction qualifies for TRA exemption?

Apply/allow TRA exemption

Transaction qualifies for low value exemption?

Apply/allow low value exemption

Apply SCA Challenge

Apply trusted beneficiaries exemption

Apply secure corporate exemption

- The TRA exemption should be the first choice for qualifying standard transactions
- Application of the low value exemption is only viable for transactions submitted direct to authorization as the ACS will not have visibility of the cumulative transaction count and value for transactions submitted via 3DS
- The Issuer should apply RBA to all transactions and has the right to still apply SCA when an Acquirer exemption is applied or the trusted beneficiaries or secure corporate exemption is indicated, if the transaction is high risk
- The trusted beneficiaries exemption may only be applied by the Issuer, but if the transaction qualifies and the merchant would like it applied, the merchant must indicate this to the Issuer
- Transactions originating in a secure corporate environment must be flagged by the Acquirer using the secure corporate payment exemption indicator unless a virtual or lodged card is used
- Issuers should note that the indicator may not be present when virtual or lodged cards are used and should check the BIN range to determine card type before taking an SCA decision
- 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

Optimising risk screening and supporting application of the TRA exemption

Issuers should carefully monitor fraud rates against the reference fraud rate thresholds to ensure they achieve a balanced application of SCA that enables them to maintain fraud rates within their target level for application of the exemptions while minimizing customer friction. Visa offers Issuers the VCAS ACS platform which utilises sophisticated risk engines to assess transaction risk.

Supporting the Trusted Beneficiaries Exemption

Supporting smooth card transactions with identified trusted merchants provides clear benefits to both cardholders and merchants, notably for transactions that would not qualify for the TRA exemption. Visa strongly encourages Issuers to support the trusted beneficiaries exemption and promote and explain it to their cardholders, who may then prefer to use a card that allows them to take advantage of the exemption over a card that does not. The Visa Trusted Listing Program provides Issuers with a complete solution to support the exemption. Issuers and their ACS providers will need to be EMV 3DS 2.2 ready to accept Visa Trusted Listing requests from participating merchants.

Visa Trusted Listing (VTL) – Issuer benefits

The **Visa Trusted Listing Program** provides a complete hosted solution for Issuers minimizing the development and operational overhead associated with offering a trusted beneficiaries solution. It facilitates addition of merchants to a customer's Trusted List, both in and outside of the purchase experience. It also supports the customer and the Issuer with the management of the Trusted List, including removal of a merchant from the list at the request of a customer.
For more information, please refer to the *Visa Trusted Listing Program Implementation Guide*.

Please note that Issuers may still choose to apply SCA to a transaction with a listed merchant, if they consider that transaction at risk of fraud.

Supporting the secure corporate payments exemption

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 are therefore encouraged to demonstrate to NCAs that applicable processes and protocols meet the requirements of the regulation and, to the extent they have met the regulatory requirements, support the exemption. They should:

- Apply the exemption when a transaction is received with the secure corporate exemption indicator – this will be the case when a merchant is indicating the transaction originated from a secure corporate purchasing system or travel management system
- Where consistent with the regulator's requirements for application of the exemption, apply the exemption where a transaction initiated by a corporate customer uses a virtual or lodged card. Note that when a transaction is processed using a virtual or lodged card, the secure corporate exemption indicator may not have been populated by the merchant/Acquirer so Issuers are expected to always check the BIN range to determine the card type before taking an SCA decision.

Additional guidance will be available from Visa in summer 2020 as to the conditions governing the use of the secure corporate payments indicator.

Issuers should not (systematically) challenge transactions flagged with an exemption

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

Visa Rule:

In line with Rule ID#0029326, Visa Issuers are reminded that they must not systematically challenge transactions sent to authorization with an

Delegated Authentication

PSPs can outsource operational functions of payment services, including the application of SCA, to a third party. The Visa Delegated Authentication (VDA) Program facilitates the delegation of the authentication process through the Visa rules, enabling Issuers to outsource authentication to third parties that are eligible to participate in the program, and thereby optimising the authentication process when SCA is required by utilising merchant / token requestor authentication capabilities.

Issuers are automatically opted in the VDA Program and are encouraged to ensure they have their authorization policies in place to support this. Issuers may opt-out of the VDA Program at any time. If an Issuer chooses to opt-out, Delegates cannot perform SCA on behalf of that Issuer under the Program. Before choosing to opt-out, we strongly encourage Issuers to first reach out to Visa to discuss the benefits of the Program and see if any actions can be taken together for the Issuer's ongoing participation in the Program.

Merchants and Token Requestors who have invested in their consumer authentication capabilities and can demonstrate best-in-class performance in managing fraud may be able to qualify for the Visa Delegated Authentication Program. In the first instance, Merchants should contact their Acquirers for further information, Token requestors should email DelegatedAuthentication@visa.com.

Summary of Visa's risk management and SCA products

Visa enables merchants, Acquirers and Issuers to minimise fraud and SCA friction as described in this guide by offering a comprehensive suite of SCA products.

Visa risk & SCA exemption management products

Merchant & Acquirer Products | Issuer Products

Fraud rate reduction

Visa Pre-dispute Products:

Merchant & Acquirer Products		Issuer Products	
Verifi Order Insight	**Rapid Dispute Resolution**	**Order Insight Digital**	**Visa Resolve Online**

Enable pre-emption & rapid resolution of disputed transactions reducing fraud rate

Exemption optimisation

3-D Secure

EMV 3DS supports better integration between the checkout and SCA challenge process as well as providing the core capability to request & apply SCA

Visa Authorization System

Allows merchants/Acquirers to submit transactions direct to authorization, flagging out of scope or exemption application status and allows Issuers to request SCA if required

CyberSource Decision Manager

Risk assesses transactions and supports exemption application & routing decisions

Visa Consumer Authentication Service (VCAS)

Supports Issuers in the application of exemptions

Visa Trusted Listing

Enables Issuers to offer the trusted beneficiaries exemption to customers shopping with participating merchants

Delegated Authentication

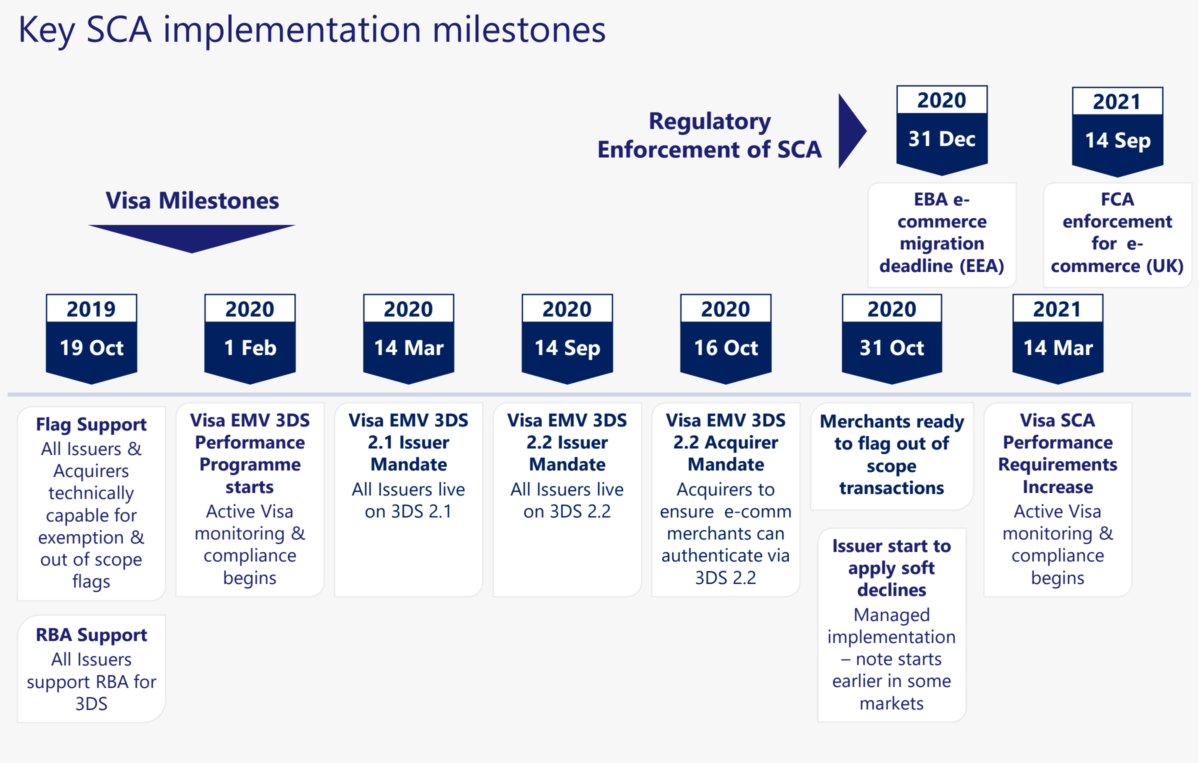
Visa Delegated Authentication Program

Facilitates Issuers with the delegation of the application of SCA to qualifying third parties, enabling them to offer their customers a consistent user experience

Timescales and Mandates

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 and has set a deadline of 31 December 2020 by which time the period of supervisory flexibility should end. While the majority of National Competent Authorities (NCAs) will align with the EBA's guidance, PSPs should ensure they act in accordance with guidance or additional conditions imposed by local regulators. The UK's Financial Conduct Authority (FCA) will start to enforce the regulation for e-commerce transactions from 14 September 2021 (subject to compliance with phased implementation plans). The migration plans of PSPs, including the implementation and testing by merchants should also be completed by 31 December 2020.

Visa has put in place a set of rules and mandates for Issuers to support 3DS 2.1, 3DS 2.2, Biometric authentication solutions and Risk Based Authentication. The key timescales are:



Key SCA implementation milestones

Regulatory Enforcement of SCA

2020 31 Dec – **EBA e-commerce migration deadline (EEA)**

2021 14 Sep – **FCA enforcement for e-commerce (UK)**

Visa Milestones

2019 19 Oct – **Flag Support** All Issuers & Acquirers technically capable for exemption & out of scope flags; **RBA Support** All Issuers support RBA for 3DS

2020 1 Feb – **Visa EMV 3DS Performance Programme starts** Active Visa monitoring & compliance begins

2020 14 Mar – **Visa EMV 3DS 2.1 Issuer Mandate** All Issuers live on 3DS 2.1

2020 14 Sep – **Visa EMV 3DS 2.2 Issuer Mandate** All Issuers live on 3DS 2.2

2020 16 Oct – **Visa EMV 3DS 2.2 Acquirer Mandate** Acquirers to ensure e-comm merchants can authenticate via 3DS 2.2

2020 31 Oct – **Merchants ready to flag out of scope transactions**; **Issuer start to apply soft declines** Managed implementation – note starts earlier in some markets

2021 14 Mar – **Visa SCA Performance Requirements Increase** Active Visa monitoring & compliance begins

Useful References

More detailed information can the subjects covered in this guide can be found in the following documents

Document/ Resource	Version/ Date	Description
PSD2 SCA for Remote Electronic Transactions Implementation Guide	Version 2.0 November 2019	Detailed Guide covering all aspects of planning for and managing the implementation and application of PSD2 SCA for remote electronic transactions.
EMVCo 3-D Secure Specification	V2.2.0	Specification for the core 3DS technology that includes message flows, field values etc. available at: https://www.emvco.com/emv-technologies/3d-secure/
Visa EMV 3DS 2.2.0 Implementation Guide	V0.1., 30 October 2019	Provides a summary of the new features of EMV 3DS 2.2 and guidance on how to use them.
Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure	Version 1.1, 21 August 2019	The Visa Secure Merchant/Acquirer Implementation Guide for EMV 3-D Secure contains operational guidance for Merchants and Acquirers on the Visa implementation of 3-D Secure. This version has been updated specifically to cover EMV 3DS 2.2.
Implementing Strong Customer Authentication for Travel and Hospitality	Version 1.1 11th March 2019	Provides merchants and Acquirers with examples of performing SCA across common payment use cases common in the travel and hospitality sectors.
Visa Secure Program Guide – Visa Supplemental Requirements	Version 1.1 8th August 2019	This document is for Visa Secure and its use to support authentication of payment transactions
Visa Secure Cardholder Authentication Verification Value (CAVV) Guide	Version 3.0 April 2019	Provides detailed information on CAVV creation and verification and use in authorization for both 3DS 1.0 and EMV 3DS.
PSD2 Strong Customer Authentication for Remote Electronic Commerce Transactions – European Economic Area: Visa Supplemental Requirements	Version 1.0 October 2019	Guide summarising Visa rules relevant to the application of PSD2 SCA.

Document/ Resource	Version/ Date	Description
Visa Delegated Authentication Program Implementation Guide	Version 1.0 5th April 2019	Describes the Visa Delegated Authentication Program and provides practical guidance to Issuers, Acquirers, technology providers, Delegates, and potential Delegates who participate in the Program on implementation and usage of the solution.
Visa Trusted Listing Program Implementation Guide	Version 1.0 9th April 2019	Describes the Visa Trusted Listing Program and provides practical guidance to Issuers, Acquirers, technology providers, and Merchants who participate in the Visa Trusted Listing Program on implementation and usage of the solution.
Visa Technology Partner Portal	N/A	Portal with additional resources including details on EMV 3DS available at: https://technologypartner.visa.com/Library/3DSecure2.aspx
Visa 3DS 2.0 Performance Program Rules	VBN 25th October 2018	Summary of Visa requirements and rules on Issuers, Acquirers and merchants for implementation of EMV 3DS
3DS Performance Rules FAQ		Summarises Visa Performance Program rules for Issuers and Acquirers
Visa Business News: Important Changes to 3-D Secure Rules to Support Strong Customer Authentication Compliance	5 September 2019	VBN stating Visa requirements for the implementation of EMV 3DS.
Strong Customer Authentication: Communication on improving outcomes from 3DSecure – Data Consistency	2 July 2020	UK Finance communication describing common errors in population of 3DS data fields and steps merchants should take to ensure key fields are correctly populated. Available at: https://www.ukfinance.org.uk/system/files/Strong%20Customer%20Authentication%20-%20Communication%20on%20improving%20outcomes%20from%203DSecure%20–%20Data%20Consistency_1.pdf