

Payments Optimisation

Elavon TRA

Transaction risk analysis up to €500

Maximise sales and security. Minimise fraud and friction



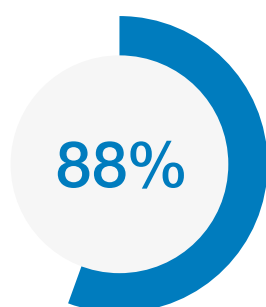
Take control: optimise your online payments

Strike a balance between sales conversion, customer experience and fraud prevention

Online payments are a prime target for fraudsters. [European card fraud](#) totalled

€1.49bn in 2020

In the UK, eCommerce online card fraud represented



[of the remote purchase fraud total](#) in 2020, linked to the increasing use of cards for online payments. Fraud levels are expected to rise still further, with researchers predicting a 53% increase in [global annual card fraud losses](#) between 2021 and 2030.

To better protect cardholders from fraud, payment service providers and merchant businesses in Europe are required to support Strong Customer Authentication (SCA). SCA reduces fraud, as shoppers must prove they are the genuine named cardholder, using at least two authentication factors:

- Something the user knows, such as a password or code;

- Something the user possesses, such as their card or phone;
- Something the user *is*, also referred to as inherence, such as a fingerprint.

Early studies [show positive results from active SCA enforcement](#), with issuers seeing a 33% reduction in the average value of [fraudulent card transactions](#) between December 2020 and April 2021.

However, SCA can also impact the consumer journey by introducing friction, with the potential to increase cart abandonment and lost sales as shoppers bail-out at the checkout.

Our payments optimisation insight will help you streamline the shopper checkout experience, to maximise sales while minimising your fraud risk. This white paper explores the opportunities offered by SCA – and its exemptions – and examines ways to minimise its impacts on your business and customers.

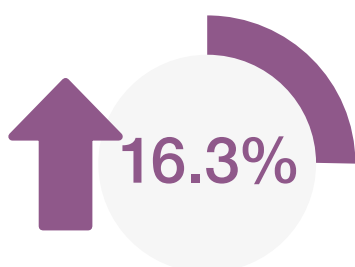
Elavon provides transaction risk analysis (TRA) support to help you leverage acquirer TRA exemption from SCA for qualifying, low-risk transactions. This exemption means your customers can enjoy a speedy, frictionless checkout experience. Find out how you can take control and find the right balance for your business between sales conversion, customer experience and fraud prevention.

Contents

04	The growth of online shopping and increases in eCommerce fraud	21	Protect your business from fraud while minimising the need for SCA: Elavon TRA
06	The online fraud challenge	21	Acquirer TRA exemption: Elavon product offerings
07	Customer feedback: easyJet	22	Outsource TRA – the service for merchants with their own risk-analysis tool
08	The Elavon model for payments optimisation and cost reduction	23	Elavon TRA – a fully managed service
	Real-time transaction risk analysis and SCA	25	Elavon TRA – How does it work?
	11 What is PSD2?	27	Impact of SCA for Elavon customers operating outside Europe
	11 What is SCA?	28	Customer feedback: Magix
13	Customer feedback: PUMA	29	Key factors in minimising SCA on customer transactions
14	Implementing SCA for card payments: EMV 3-D Secure	31	Why request the TRA exemption?
	What does SCA mean for my business?	32	Finding your balance
	16 Maximise sales by streamlining the consumer experience	34	Take best advantage of the ways SCA can work for you
	16 Remote low-risk transactions – key facts about TRA exemption	35	Frequently asked questions

The growth of online shopping and increases in eCommerce fraud

It is estimated that in 2021, worldwide retail eCommerce sales grew



While worldwide in-store sales also grew in 2021 (8.2%), as brick and mortar retailers recovered from the impact of COVID in 2020, online sales have continued to play an increasingly important role. Retail eCommerce sales as a percentage of total retail sales grew from 17.9% in 2020, to 19% in 2021.

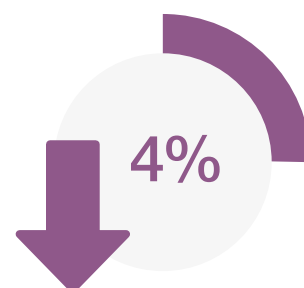
The growth of online commerce as a percentage of total retail sales is striking. Researchers forecast that by 2025, eCommerce will make up close to a quarter of total worldwide retail sales. Even as growth rates slow, total worldwide eCommerce retail sales are predicted to exceed \$7 trillion by 2025.

In the UK, the changing ratio has been even more pronounced. In January 2021, internet sales accounted for 36.3% of total retail sales, representing a 22.1% shift online in five years. There has also been a shift from desktop to mobile: in 2021, some 75% of all online transactions were carried out on mobile devices, largely (79%) through full service native mobile apps.

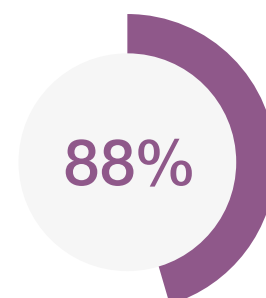
This rapidly evolving and competitive landscape offers many benefits to consumers, such as convenience and greater choice, but it also presents more opportunities for fraud.

Research found that in 2019, card fraud across Europe reached €1.55bn. While fraud losses dropped in 2020, to €1.49bn, only 5 of the 18 European countries included in the study achieved card fraud reductions, the remaining countries (including France and Germany) showed an increase or no reduction in fraud losses.

In the UK, total remote purchase (card-not-present) fraud (internet, telephone or mail order) also reduced in 2020, by 4%.



However in the same period, an estimated £376.5 million of eCommerce online card fraud took place, a 4% increase (88% of the remote purchase fraud total).





Globally, financial loss caused by payment fraud tripled from

\$9.84bn

in 2011



\$32.39bn

in 2020

Between 2021 and 2025, online payment fraud is expected to result in more than \$206bn. of merchant losses. Other researchers, looking further ahead, predict that by 2030 global annual card fraud losses will reach an estimated

\$49.32bn

The real cost of fraud to you, as an online merchant, is greater than just the direct monetary value lost through fraudulent transactions; there are many other operational costs and losses, such as chargebacks, legal costs and merchandise replacement.

In its 2021 True Cost of Fraud Study, LexisNexis Risk Solutions found that US online retail merchants incurred

\$3.60

costs for every

\$1

of fraud committed, compared to \$3.36 in 2020

The online fraud challenge

Online transactions can present more challenging scenarios than in-store purchases, especially with liability concerns when fraud occurs. Online payments are a prime target for criminals: the ready availability of large volumes of compromised card details on the dark web, and often the associated customer personal details, enables fraudsters to commit online financial crime with very little effort.

Businesses like yours need to take steps to prevent many types of fraud – not just from criminal fraudsters, but also from so-called ‘friendly fraud’.

Criminal fraudsters:

- Misuse of stolen payment card details;
- Synthetic ID theft fraud (legitimate card details issued to a ‘synthetic’ person);
- Account takeover fraud (fraudsters use legitimate customer credentials to order goods);
- Refund fraud (customers try to get money back for goods for which they didn’t pay);
- Triangulation fraud (the innocent customer makes a genuine purchase on a third-party marketplace; the goods they receive were purchased by the fraudulent marketplace seller using stolen card details from a legitimate retailer’s website).

Friendly fraud:

- Chargeback abuse (e.g. item not delivered);
- Buyer’s remorse;
- Familial fraud (purchases made on family accounts);
- Confused customers disputing already refunded transactions.



You naturally want to take advantage of the growing online market, but you also need to be able to distinguish genuine customers and legitimate card transactions from criminal fraudsters –

In order to:


- ↙ ↘ ↗ ↖ Minimise fraud losses
- 📦 Reduce operational costs associated with fraud prevention and chargeback management

Studies have shown that online merchants can spend almost a quarter (23%) of their operational budget on fraud prevention and chargeback management.

One 2021 Global Fraud Survey found that surveyed merchants spent around 10% of their annual eCommerce revenue on fraud management.

While also:

- 🛒 Maximising sales opportunities
- 🧠 Limiting the impact on your customer experience
- 💰 Increasing conversion rates



“Elavon demonstrated an early appreciation for the potential impact of PSD2 and SCA on the travel industry, bringing together airlines and partners to share knowledge and ensure readiness for SCA well before the enforcement deadlines.

“TRA exemption for transactions up to €500 has been key to easyJet maximising transaction approval rates while minimising customer friction and abandonment... authorisation levels remain high, with no negative effect on our fraud rates.”

Paul Bolton
Head of Payments, easyJet



The Elavon model for payments optimisation and cost reduction

To help you address this need, Elavon has leveraged Featurespace, a world leader in fraud prevention, to develop our advanced fraud services.

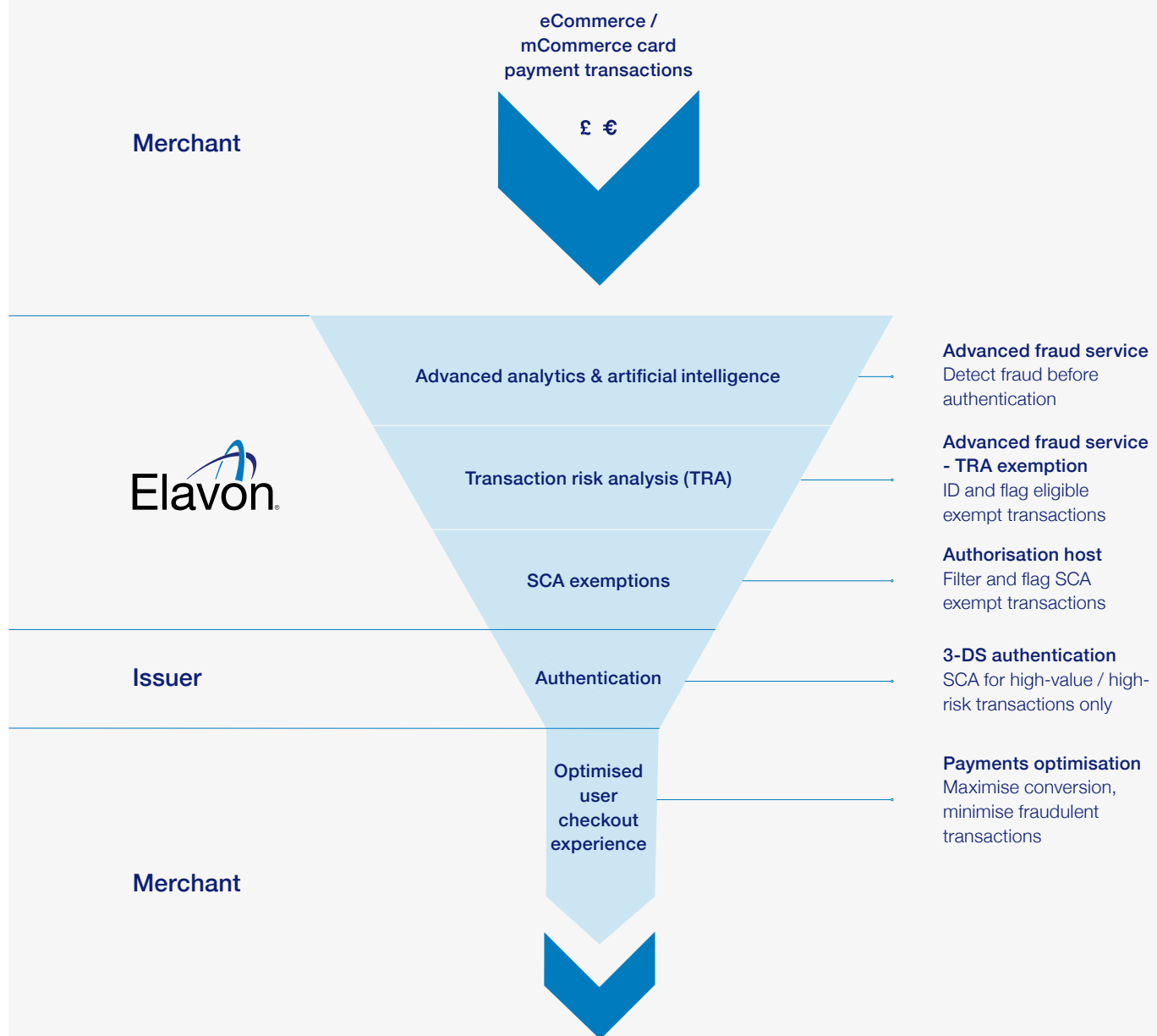
The advanced fraud services at Elavon will serve to protect your customers and your business from fraudulent transactions by making best use of **artificial intelligence (AI)** and **advanced analytics**.

The industry-leading fraud detection and prevention capabilities of our advanced fraud services will:

- ✔ Help you tackle fraud attacks in real time;
- ✔ Reduce chargeback rates while removing the need to review transactions manually;
- ✔ Simplify the online checkout experience for your customers;
- ✔ Positively impact gross revenue.

A solution that you will be able to employ to deliver payments optimisation, as shown in the diagram below:

- Uses advanced analytics & artificial intelligence so fraud can be detected before authentication and authorisation.
- Request exemption from SCA (acquirer TRA exemption) for eligible transactions. (See next section for more details: 'Real-time transaction risk analysis and SCA', p9).
- For quicker transaction times that streamline your customers' checkout experience, maximising shopping cart conversion and increasing online sales.



*taken from 'PSD2 & Strong Customer Authentication: What Acquirers Need to Know'
 †based on Visa risk-based authentication case study "Frictionless Experience with Verified by Visa."



Real-time transaction risk analysis and SCA



The fraud-detection capabilities of Elavon also support our transaction risk analysis (TRA) risk engine: Elavon TRA.

Elavon TRA enables you to make the most of the benefits of SCA, which is required by the European Union's Payment Services Directive 2 (PSD2).


- Elavon TRA is performed in real time with an instant response that doesn't extend the processing time of the payment transaction.
- The Elavon TRA risk engine will assess each transaction using significantly more data for each transaction than is available to the card issuer.
- Elavon TRA can help to control the potentially negative impacts of SCA and, most importantly, protect both you and your customers in equal measure.

What is PSD2?

PSD2 set out to:

-  **Make payments safer and more secure**
-  **Protect cardholders and merchant businesses from payment fraud**

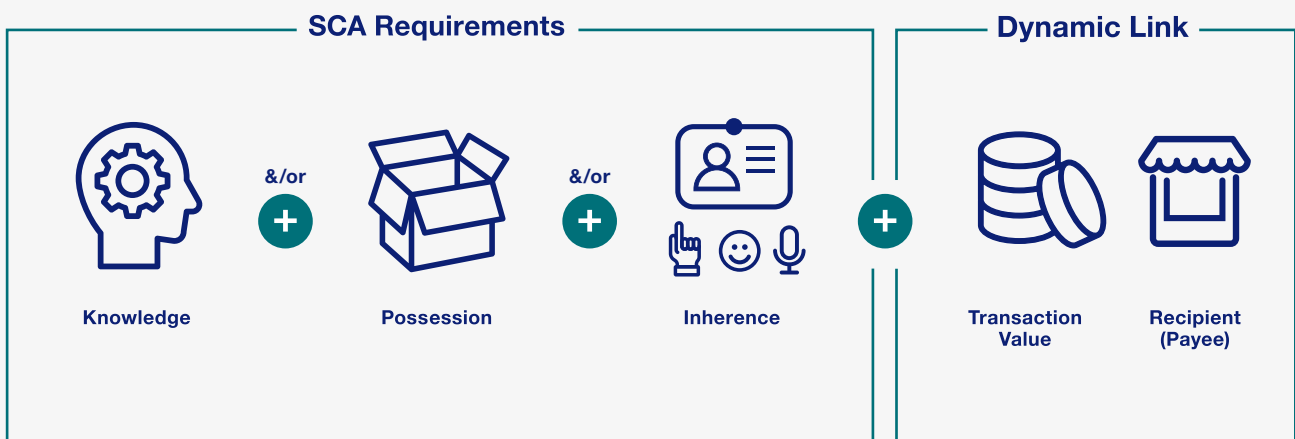
The technical standards of PSD2 require the application of SCA for any electronic payments or other risky remote consumer actions, such as setting up an electronic payment mandate.

 **For more information on PSD2, see our dedicated [PSD2 hub](#).**

What is SCA?

SCA is an authentication process that validates the identity of the shopper, proving they are the genuine cardholder, based on the use of at least two independent authentication factors. Successful authentication must result in the generation of an authentication code.

All cardholder-initiated remote electronic payment methods are in scope, including online (eCommerce, mCommerce) and mobile in-app payments. SCA must be performed before any funds are authorised and transferred; the authentication code generated must be specific to the amount of the payment transaction and the payee, a 'dynamic link':



The original enforcement date for SCA was from 14 September 2019. However, significant concerns about the state of readiness of the payments industry, the potential impact on payments and the risk of negative consequences for cardholders led to the European Banking Authority (EBA) postponing enforcement of SCA for eCommerce transactions:

Location of card issuer	SCA enforcement date
EEA countries ¹	31 December 2020
United Kingdom	14 September 2021

With the SCA enforcement deadline now passed, card issuers based in the European Economic Area (EEA), most card issuers must now apply SCA for all in-scope eCommerce payment card transactions (unless the transaction can be exempted from SCA).

The Payments Association reported that, post-December 2020, SCA enforcement did not result in mass consumer disruption or significant cart abandonment.

That online retailers have not experienced a Europe-wide mass decline of transactions is largely due to the individual countries' national competent authorities (NCAs) taking a staged or gradual ramp-up approach to full SCA enforcement. During these periods of 'soft enforcement' entities across the payments ecosystem monitored authentications, authorisations and use of exemptions, identifying and addressing technical issues as well as educating merchants and cardholders in preparation for the full enforcement of SCA. As these periods of flexibility have all now passed, merchant businesses must take a proactive approach to understand how SCA is impacting their online payments and to minimise

any negative impacts of SCA on their customers and sales. Merchants, working with their acquirers and payment service providers, need to ensure they fully support SCA authentication mechanisms, correctly flag out of scope transactions, take advantage of applicable SCA exemptions and monitor for and take steps to address excessive authentication abandonment or issuer soft declines.



¹ EEA countries are all 27 EU member states plus Iceland, Liechtenstein and Norway.

“TRA provides PUMA with a technical approach to optimise our payment strategy and customer experience, keeping the authorisation rates high while reducing friction for payments rated as low risk.”

Marcus Riese

Senior Payment Specialist E-Commerce Europe
PUMA



Implementing SCA for card payments: EMV 3-D Secure

The industry standard tool for SCA is EMVCo's 3-D Secure messaging protocol. 3-D Secure enables the issuer to verify the identity of the cardholder making the online purchase – not only protecting the cardholder from fraudulent use of their payment card details, but also protecting you and your business from fraudulent chargebacks.

Many merchants are understandably wary of 3-D Secure after poor experiences with its previous iteration, 3-D Secure 1. However, compared to 3-D Secure 1, the latest version, EMV 3-D Secure (3-D Secure 2.2), incorporates a number of enhancements.

3-D Secure 2.2:

*****_** Offers a better customer experience and doesn't rely on customers remembering a static password for authentication.



Supports multiple options for SCA, including one-time passcodes, as well as biometrics via out-of-band (OOB) authentication flows. OOB allows for issuer authentication of the cardholder to occur outside the merchant shopping environment, for example via push notification to the cardholder's banking app.



Supports modern technologies and payment methods: in-app, mobile and digital wallets.



Supports SCA exemption flagging including the acquirer transaction risk analysis exemption.

x10

Supports ten times more data points, which can contribute to increased fraud detection and a frictionless customer experience.



EMV 3-D Secure has the capability to offer a frictionless authentication flow where, for low-risk transactions, the customer is authenticated with no interaction. This risk-based authentication by the issuer utilises the additional data points captured during checkout and transaction history data.

However, **frictionless authentication is not possible for all transactions.** The application of SCA may increase the risk of cart abandonment, due to the potential for friction in the 3-D Secure authentication challenge flow.



As card issuers are required to apply SCA, it is therefore critical that you take advantage of all available options to enhance the frictionless customer experience and maximise the volume of transactions that do not require SCA challenge – thereby maximising sales success.



3-D Secure authentication adds to overall transaction time. Analysis by [Ravelin](#) found that 3-D Secure authentication took an average of 37 seconds.



February 2022 figures from Visa showed a UK average challenge success rate of ~82%². While in the wider EEA, 9 months after the SCA enforcement deadline, [failure rates on transactions](#) being challenged through 3-D Secure 2 were at 29% (European weighted average)



[Elavon research](#) revealed that two-thirds of cardholders will abandon an online purchase made on a mobile device if the process is too difficult.



Longer, more complex checkout processes may lead to increased cart abandonment. A recent [checkout research study](#) found that, over a three-month period, one in five shoppers abandoned their shopping cart due to a *“too long/complicated checkout process”*.

What does SCA mean for my business?

Card issuers must apply SCA for all eCommerce payment transactions, unless the transaction is out of scope for PSD2 or can be exempted from SCA.

It is not only card issuers that need to support the 3-D Secure authentication mechanism – so too do all other entities involved in the payment transaction: merchants, payment gateways and acquirers. Although issuers are the regulated bodies specifically obliged to apply SCA to their cardholders, these other entities need to support 3-D Secure in order to:



Minimise disruption caused by SCA enforcement;



Maximise frictionless transactions;



Maximise conversion and online payments growth.

Maximise sales by streamlining the consumer experience

Conversion and growth can be driven by minimising the friction that cardholders experience at the point of payment. There are opportunities to streamline and reduce friction at two stages in the cardholder payment journey:

Stage 1: Minimise the need for SCA to be applied to a transaction

Cardholder authentication is not required for transactions that:

- Are out of scope for PSD2;
- Can be exempted from SCA.

Stage 2: Offer a seamless cardholder SCA experience as and when SCA is required

Streamlining the cardholder SCA experience is primarily the responsibility of card issuers. Issuers need to:

- Apply risk-based analysis in order to avoid challenging transactions unnecessarily;
- Adopt SCA solutions that minimise friction by maximising the use of biometrics/behavioural biometrics;
- Apply issuer exemptions for qualifying transactions.

Your role in reducing cardholder friction by minimising the need for SCA to be applied (at Stage 1 [p15]).

SCA is required for online payments, unless the transaction is out of scope for PSD2 or can be exempted from SCA:

In scope for SCA		Out of scope
Available SCA exemptions		
Acquirer PSPs	Issuer PSPs	<p>Unattended transport fares and parking fees</p> <p>Anonymous pre-paid transactions</p> <p>Payments initiated by mail or telephone (MOTO)</p> <p>'One-leg out' transactions³</p> <p>'One-leg in' transactions⁴</p> <p>Merchant initiated transactions (MITs)⁵</p>
<p>Low-value remote electronic payment transactions</p> <p>Payments €30 or below; issuer counter limit: €100 cumulative spend or five consecutive transactions</p>		
<p>Recurring transactions</p> <p>of the same amount and to the same merchant</p>		
<p>Transaction risk analysis (TRA)</p> <p>For low-risk transactions if PSP fraud rate within specific thresholds, depending on transaction amount. Audited transaction risk-monitoring mechanisms must be in place to enable real-time risk analysis and risk scoring</p>		
	Payments to trusted beneficiaries	
	Secure corporate payments	

³ One-leg out: the merchant's Payment Service Provider (PSP) - their Acquirer - is located outside the EEA or UK. SCA performed on 'best efforts' basis.

⁴ One-leg in: the cardholder's PSP (the Issuer) is located outside the EEA or UK; the issuer is not subject to PSD2

⁵ MIT: payments initiated by the merchant without any direct intervention from the cardholder are excluded, if the merchant has valid authority (mandate) from the consumer.

You should seek to leverage the opportunities offered by the defined SCA exemptions and scope to minimise the negative impacts of SCA on your business and your customers.

Of the SCA exemptions available to you (via your acquirer, Elavon), the **acquirer TRA exemption** should be your first choice⁶. This recommendation is borne out in the exemption usage seen in the market since 1 January 2021; across Europe, the TRA exemption is being applied as the preferred exemption flag.*

The **low-value SCA exemption** is not recommended as your first choice, as the acquirer/merchant has no view of the cumulative spend or consecutive transaction counts; the transaction will need to be resubmitted for SCA via 3-D Secure if either limit is reached.

The SCA **recurring transactions** exemption is limited to payments of the same amount to the same payee – and SCA is required when the series of payments is established or amended. For greater flexibility, it is recommended that recurring transactions are processed as merchant-initiated transactions (MITs) which are out of scope.

Note that the card issuer always makes the final decision on whether to accept or rely upon an SCA exemption. Issuers may choose not to honour the requested exemption; they may instead respond with a soft decline ('step-up').

*Mastercard 2021 Week 3 (starting January 18th) Authorisation data had the TRA exemption share at 51% for Authorisation Exemptions/Exclusions (TRA vs. low-value vs. MIT vs. recurring payments) [Mastercard PSD2 RTS Readiness Status and Heightened Awareness Update, 29 January 2021]

Visa Heightened Awareness call 3 February 2022: TRA exemption was the most used at 27% of total UK e-com volumes; low-value exemption was at 5%.

Remote low-risk transactions – key facts about TRA exemption

The TRA exemption may be applied for remote low-risk transactions, where no risk factor is identified for the payment by the PSP's risk-monitoring mechanisms. These include: abnormal spending or behavioural patterns, unusual information about the payer's device/software access, malware infection, abnormal location of payer or high-risk payee location.

Acquirer TRA exemption:

- Your acquirer can apply the SCA TRA exemption; if they do, fraud liability shifts to the acquirer (and hence to the merchant) instead of the issuer.
- An acquirer TRA exemption request may be overridden by the issuer. Issuers may 'step-up' to request authentication, rather than accept the exemption request.
- The acquirer's fraud rate is critical to TRA exemption:

Acquirers with lowest overall fraud rates can apply TRA exemption for their highest value transactions:

- Acquirers with reference fraud rate of **0.01%** or less can apply for TRA exemption for transactions up to €500.
- Acquirers with reference fraud rate of **0.13%** or less can apply for TRA exemption for transactions only up to €100.
- Above €500, SCA is always required, unless one of the other SCA exemptions with no transaction value limit can be applied (e.g. transaction is a recurring payment or the merchant is already listed with the account servicing payment service provider (ASPSP) as a trusted beneficiary.) The ASPSP is the financial institution that provides and maintains the customer payment account – this includes banks, card issuers and building societies.

Exemption threshold value (ETV)

Acquirer fraud rate

€500 €250 €100

≤ 0.01% ≤ 0.06% ≤ 0.13%

In December 2021, the average order value across all eCommerce markets was £81.14. An indication that the majority of online retailers could significantly benefit from Elavon TRA's ability to offer a frictionless checkout experience for their customers.





The reference fraud rate at Elavon is currently less than 0.01%, **allowing us to apply TRA exemption for customer transactions up to €500** (or equivalent).*

*Elavon will apply the TRA exemption to qualifying low-risk transactions for eligible customers set-up for 'Elavon TRA'



Your role in the cardholder SCA experience (at Stage 2 [p15])

To support issuers' application of SCA for cardholder-initiated remote electronic payments and to help increase the frictionless cardholder SCA experience, you should:

-  Implement best practices for your business profile;
-  Ensure business processes and systems support SCA for all direct sales channels accepting cardholder-initiated transactions (CITs), including both online and mobile platforms:
 -  Ensure support for the latest version of 3-D Secure (EMV 3-D Secure 2.2), and
 -  Ensure support for 3-D Secure fallback* (to 3-D Secure 1.0.1);

Note that card on file (COF) payments, triggered by the cardholder, will require SCA to be performed.

*The card schemes will cease support for 3-DS 1.0.2 from 14 October 2022.



Optimise the integration of 3-D Secure SCA challenge screens into browser and app checkout;



Ensure all required 3D-Secure data points are available for issuer evaluation to support accurate decision-making. [Analysis by UK Finance](#) identified that for 30-80% of sampled transactions three key data fields caused significant errors if they were missing, incomplete or inaccurate (Browser IP, Shipping & Billing postcode, Address match indicator);



Check for SCA support for any indirect sales channels, such as transactions accepted via third-party agents, which act as an intermediary between you and the end cardholder.

Even though EMV 3-D Secure 2.2 is specifically designed to support the minimisation of friction when SCA is required, and while SCA provides an added layer of protection for both you and your customer, it is **recommended that you do all you can to minimise the need for SCA to be applied by following the recommendations** given in this paper.

Protect your business from fraud while minimising the need for SCA: Elavon TRA

You can work with Elavon to apply the acquirer TRA exemption for all qualifying online payment transactions.

Acquirer TRA exemption: Elavon product offerings

As an acquiring bank, Elavon can offer our customers two approaches to enable application of the acquirer TRA exemption:

	Outsource TRA	Elavon TRA
What is it?	Service allowing you to request TRA exemption.	Service where Elavon requests TRA exemption on your behalf.
Relies on	You performing your own evaluation of transaction risk.	Elavon risk engine performing transaction risk analysis.
Suitable For	<p>Merchants wishing to leverage acquirer TRA exemption for eligible transactions below Elavon ETV, (see p18)</p> <p><i>and</i></p> <p>Willing to make own decision on taking on transaction fraud liability.</p>	<p>Merchants wishing to leverage the Elavon risk engine to seek SCA exemption for eligible transactions.</p> <p>Merchants willing to accept Elavon's decision on taking on transaction fraud liability.</p>
Eligibility	<p>Merchants with existing risk analysis and fraud management capability.⁷</p> <p>Able to support 3-D Secure 2 and respond to soft declines.</p> <p>Average transaction value up to €500.</p> <p>Fraud rate for most recent six months is less than 12bps (0.12%).</p> <p>Technical capability to include TRA exemption indicator in the authorisation request.</p>	<p>Able to support 3-D Secure 2 and respond to soft declines.</p> <p>Average transaction value up to €500.</p> <p>Fraud rate for most recent six months is less than 12bps (0.12%).</p> <p>Technical capability to include TRA exemption indicator in the authorisation request.</p>

⁷ Customer's risk analysis and fraud management tool must satisfy European Banking Authority criteria

Outsource TRA – the service for merchants with their own risk-analysis tool

Elavon recognises that many of our customers have invested in their own fraud-management capability and want to leverage that in-house capability to avoid 3-D Secure for their low-risk transactions below the Elavon ETV. **With Elavon Outsource TRA – you can!**

You tell us exactly which payments to flag for TRA exemption, using your own risk-rating tool. Elavon will then simply send exemption requests to the issuer.

If your fraud-monitoring solution meets the European Banking Authority's Regulatory Technical Standards criteria for TRA and is able to go through the Elavon Third-Party Risk Management process, you can apply for Outsource TRA in order to avail of the acquirer TRA exemption.

Elavon TRA – a fully managed service

Elavon will do the hard work. Our TRA SCA exemption engine analyses and profiles transactions to make the best exemption decisions for your business.

Elavon TRA is available for customers wishing to exempt qualifying transactions from SCA.

Elavon TRA is performed in real-time with an instant response. This saving in transaction latency is another reason eligible customers are encouraged to sign-up for Elavon TRA. Cardholders will experience a frictionless checkout for low-risk score, TRA-exempted transactions that are sent straight to authorisation.

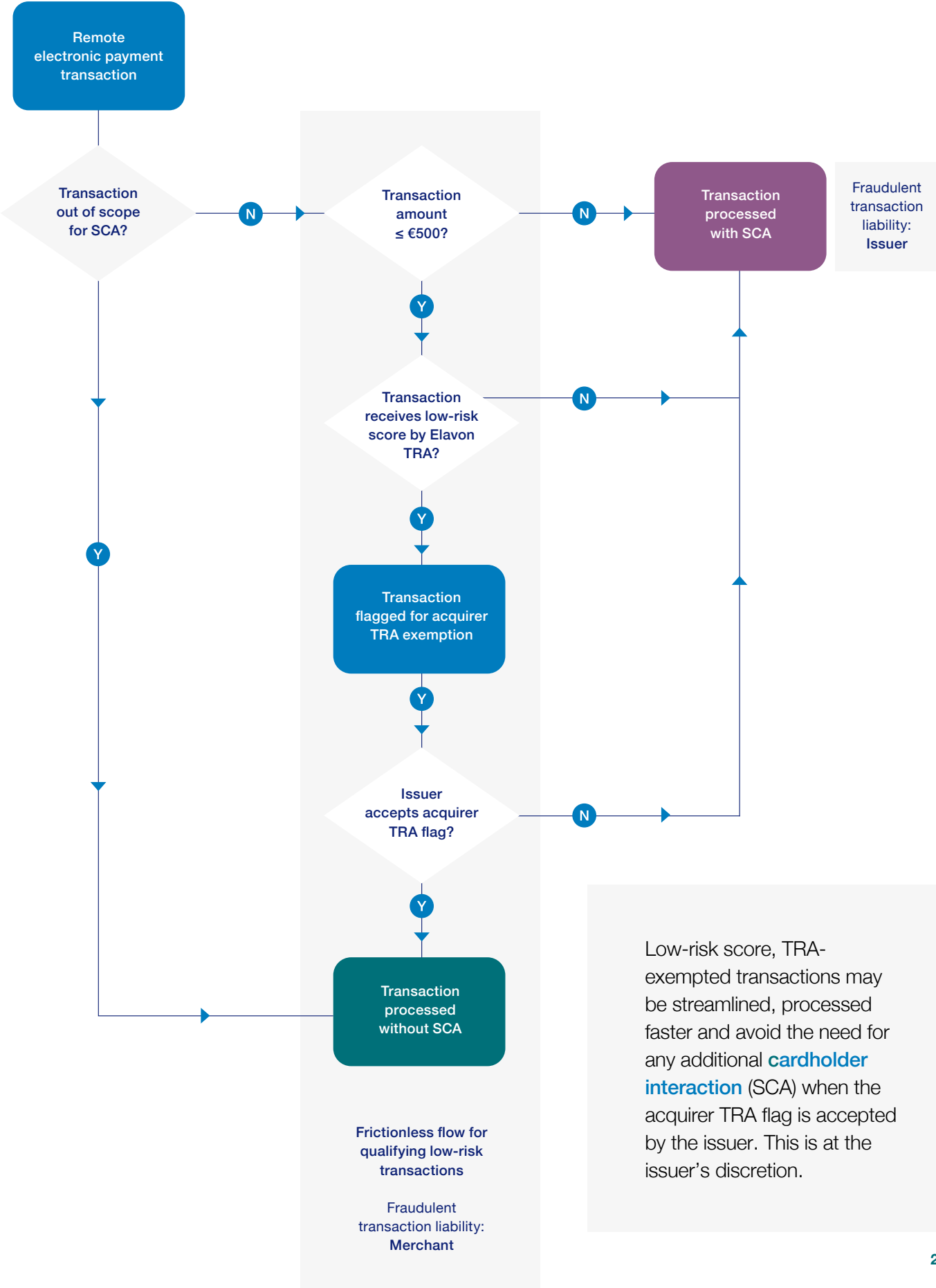
If the issuer accepts the acquirer TRA exemption request, the transaction will be processed without the need for an SCA challenge – enabling a frictionless transaction.

If the Elavon TRA service or your own tool (under Outsource TRA) assesses the transaction to be high risk, or if the issuer declines the exemption request, a soft decline ('step-up') will be initiated. A soft decline is a request for the transaction to be submitted via 3-D Secure for cardholder authentication.

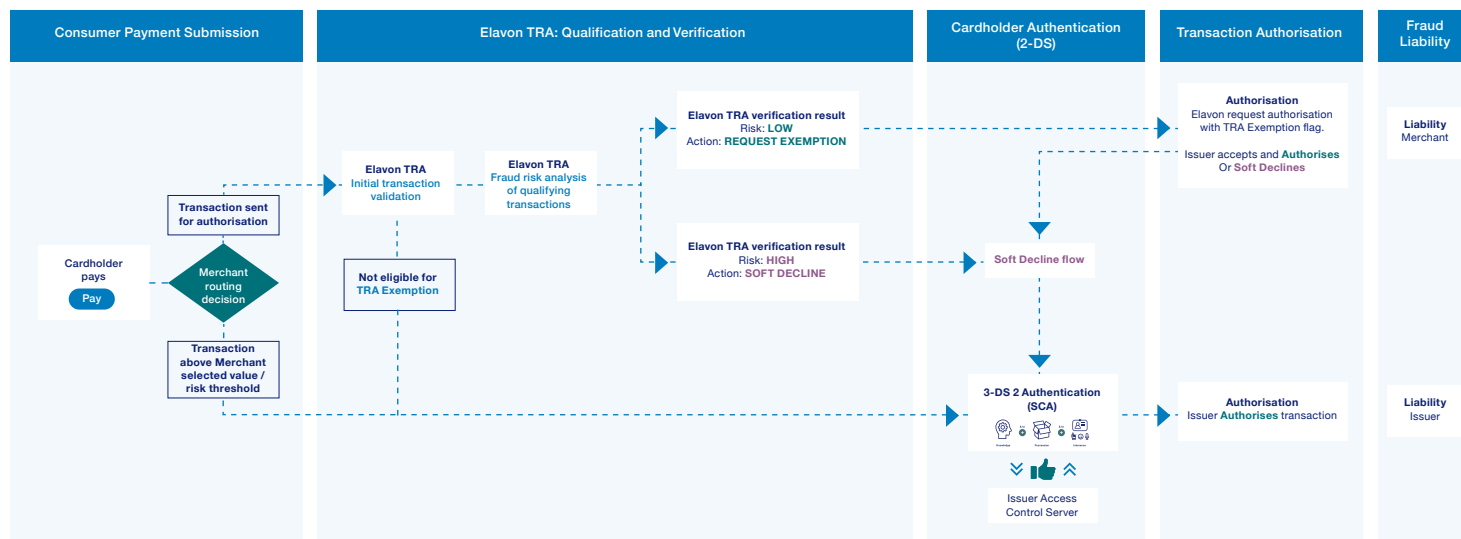
The ability of Elavon TRA to support a frictionless flow for low-risk transactions is illustrated on the following page. All in-scope, eligible transactions can be sent through the frictionless flow.



Elavon TRA: Decision Tree



Elavon TRA – How does it work?



Eligible transactions sent **straight to authorisation** with the acquirer TRA exemption flag:



For eligible transactions ≤€500 (or equivalent).



You are willing to accept fraud liability.



When Elavon TRA gives low-risk score.



Offers lower transaction latency/processing time.



No fee for authentication via 3-D Secure (unless issuer soft declines: 'step-up').

All transactions ≤€500, or a lesser value that you choose, may be qualified by Elavon TRA and flagged for TRA exemption. **Issuers will be inclined to accept** acquirer TRA exemption requests sent straight to authorisation because:

- Issuers know that Elavon will only request TRA exemption for transactions **where fraud risk is low** or risk impacting our own fraud rate (and potentially the ETV of Elavon);
- Issuers are happy **to pass on the fraud liability** to you, the merchant.

Issuers may not honour the acquirer TRA exemption; they may soft decline the transaction ('step-up'). To avoid a decline, the cardholder must be available for SCA if step-up is requested.



Early adopter Elavon TRA customers have been able to achieve up to **100% approval rates** for eligible transactions submitted with the TRA exemption request flag.

Issuers use transaction data submitted in the authentication request to assess the fraud risk of transactions submitted with the acquirer TRA exemption flag.

- If the transaction risk is low, the issuer may apply the TRA exemption **without the need to challenge** the cardholder (frictionless, risk-based authentication).
- Only if the transaction risk is high, will an SCA challenge be triggered.

A note on merchant initiated transactions:

Leveraging the acquirer TRA exemption is only recommended for one-off, cardholder-initiated payments where no future MIT is expected. A MIT is a transaction where the cardholder is not present ('off session'). The transactions are initiated by the merchant and do not require any direct intervention from or action by the payer.




MITs are governed by a prior agreement between the cardholder and merchant. A MIT must always be preceded by a cardholder initiated transaction (CIT), which may be a zero value transaction. An initial CIT is necessary for SCA to be performed and the agreement for subsequent MITs to be established. The merchant must retain the result of the SCA from that CIT, which must be submitted with all subsequent MITs.

Since 1 January 2021, the percentage of transactions flagged as MITs and therefore out of scope for SCA has been increasing.⁸ MIT transactions have, so far, been seen to have lower approval rates. Therefore, maximising use of the TRA exemption should still be your first choice.


Impact of SCA for Elavon customers operating outside Europe

SCA enforcement by EEA- and UK-based card issuers not only impacts merchant businesses operating within Europe; it may also impact those based outside of Europe.

SCA's geographic applicability is illustrated below:

In scope/ out of scope	Location of:		
	 Merchant	 Merchant Acquirer/PSP	 Card Issuer/ Consumer Bank
In scope for SCA	EEA and/or UK	EEA and/or UK	EEA and/or UK
	Outside EEA or UK		
Not in scope Best efforts (one leg out)	Outside EEA or UK	Outside EEA or UK	EEA and/or UK
Not in scope	EEA and/or UK	EEA and/or UK	Outside EEA or UK

All businesses that sell to customers holding payment cards issued within the EEA/UK and using an EEA- or UK-based acquirer for those transactions must be able to support the application of SCA. As can be seen in the table, the location of the merchant business does not influence whether the payment transaction is in scope for SCA.

A person's hands are shown holding a smartphone. The background is blurred, showing other people in a public setting. A large teal rectangular overlay covers the left and center of the image, containing white text. The text is a testimonial about PSD2 regulations and TRA, praising Elavon's security checks.

“As a creator of cutting-edge software, it’s critical that our customers can shop securely on our website. PSD2 regulations make online payments safer, but the necessary security checks can frustrate consumers. TRA makes online checkout smoother and safer without annoying our customers, resulting in approval rates of around 95%. Well done, Elavon!”

Martin Raschke

Senior Controller, Magix

Key factors in minimising SCA on customer transactions

Minimise fraud

Work to minimise misreported and ‘friendly’ fraud⁹ to prevent or resolve disputed transactions. Disputes can artificially inflate fraud counts, limiting the ability of Elavon to:

- Consider individual customers for application of TRA exemption;
- Apply the TRA exemption.

Properly identify and flag transactions

Transaction flags and authorisation indicators must be accurate and consistent in order to properly identify out of scope transactions, including:

- Mail order/telephone order transactions and
- MITs.

Visa estimates that 54% of ‘card not present’ (CNP) volume is in scope for SCA, with 13% of CNP volume yet to be flagged to reflect its out-of-scope status¹⁰.

Research conducted between September and October 2021, found that incorrect or incomplete transaction flagging resulted in failed transactions especially for MITs.

⁹ Friendly Fraud, also known as Chargeback Abuse, occurs when a legitimate customer procures a refund while retaining purchased goods or services after making a false complaint.

¹⁰ Visa - Strong Customer Authentication: Tools & Practices for Merchants/Acquirers to Minimise Customer Friction, 11 June 2020.

Apply risk-based analysis

The Elavon advanced fraud services and Elavon TRA performs risk-based analysis of transactions before submitting for authentication or authorisation. This risk screening of transactions allows:

- Fraudulent transaction to be identified prior to submission, minimising per transaction costs;
- TRA exemptions to be applied for eligible low-risk transactions.

For high-risk transactions, Elavon TRA responds with a soft decline ('step-up'); the transaction needs to be submitted via 3-D Secure for SCA.

Use 3-D Secure 2.X

All parties in a transaction need to support EMV 3-DS 2.x, while also supporting the ability to fall back to 3-D Secure 1* if the card issuer cannot support 3-D Secure.

Ensure you can follow-up any soft declines with a 3-D Secure 2.x authentication request; though properly flagging transactions will minimise the number of soft declines received.

Apply exemption strategy

An appropriate exemption strategy is about achieving a balance between:

1. Eligible transactions sent straight to authorisation with TRA exemption flag;
2. Transactions sent for SCA via 3-D Secure.

Submitting direct to authorisation can enhance the frictionless customer experience by reducing friction and minimising latency and reduce your per-transaction costs.

The main implication of applying an SCA exemption is that Elavon (and hence you, our customer) takes on the liability for the transaction and any subsequent fraud.

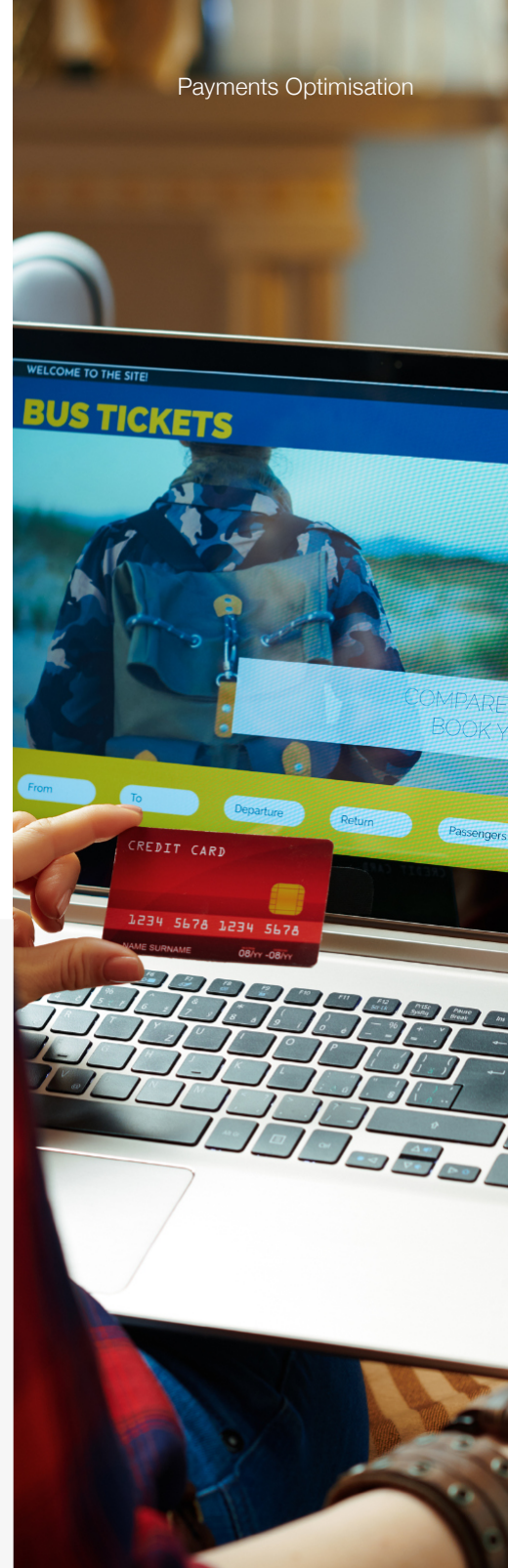
* The card schemes will cease support for 3-DS 1.0.2 from 14 October 2022.

Why request the TRA exemption?

Simply put, Elavon TRA can help you find your ‘sweet spot’ to achieve payments optimisation.

Using TRA to exempt your low-risk transactions from SCA, and authenticating higher-risk transactions via 3-D Secure, is an effective way for Elavon customers to balance sales and fraud goals: **payments optimisation.**

Payments optimisation is about balancing the desire to maximise conversion and increase sales with the need to avoid chargebacks and fraud losses.



Potential impact of SCA without payments optimisation

18%

As of November 2021, the Microsoft SCA scorecard showed that 18% (mobile app) or 12% (browser) of payments sent for 3-D Secure authentication were abandoned.

19%

While authentication success was low 66% (mobile app) or 76% (browser); showing an even greater impact than pre-enforcement analysis that 19% of payments were lost, even with the improved 3-D Secure 2 consumer experience.

29%

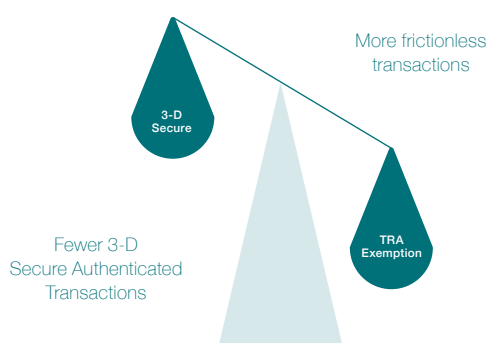
9 months after the EEA SCA enforcement deadline, failure rates on transactions being challenged through 3-D Secure 2 were at 29% (European weighted average).

Online businesses need to maximise their use of SCA exemptions to offer genuine customers a smooth journey.

Finding your balance

With low risk, average transaction values up to €500 and low fraud rate, you will be able to:

- ↑ Maximise use of TRA exemption and
- ↓ Minimise the number of transactions requiring SCA.



By using Elavon TRA, your choice of eligible, low-risk transactions will be automatically flagged for TRA exemption and sent straight to authorisation with minimal risk of increased fraud.

Your business will benefit from:

- Increased sales/conversion due to frictionless, low latency transactions.

In Q1 2022, Elavon customers leveraging the TRA exemption enjoyed an average 3.6% increase in sales as 88% of their TRA flagged transactions (on average) were approved by issuers with no cardholder challenge and with no impact on their fraud rate/chargebacks.

Detailed cost-benefit analysis using live merchant values

To demonstrate the synergies of provision of both 3-D Secure and TRA to a merchant, the following data extrapolates live processing sales, fraud and 3-D Secure values from an existing Elavon merchant, a major international retailer of sporting goods.

Scenario 1

Cost-benefit analysis maximising the volume of transactions flagged for TRA exemption

- Increase in monthly sales between €2.9 million and €7.7 million*

*Retrospective analysis showed a potential increase of €2.9 million in March 2020 and of €7.7 million in May 2020 when the retailer maximised use of the TRA exemption.

High-risk merchants with greater volume of transactions above acquirer ETV and higher fraud rates may also utilise Elavon TRA:

- Transactions above Elavon's ETV (or a lowvalue determined by the merchant) are sent for 3-DS Authentication (SCA)
- All eligible, low-risk transactions below the Elavon ETV (or merchant's chosen value) will be automatically flagged for TRA exemption and sent straight to authorisation with minimal risk of increased fraud
- Elavon TRA will respond to eligible but high-risk transactions with a soft decline ('step-up') for SCA to be applied.

For customers in this scenario:

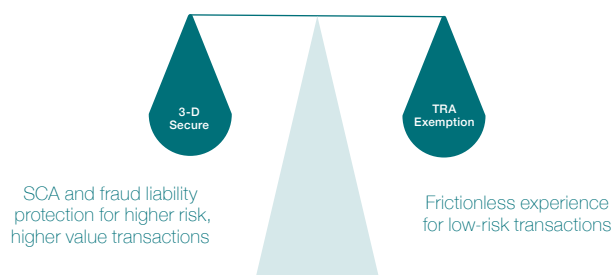
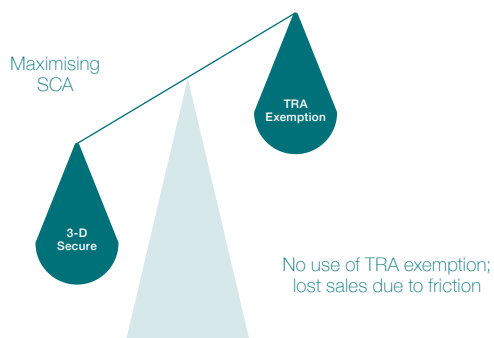
- Higher value, higher-risk transactions will be submitted for authentication, giving the merchant fraud liability protection and minimising unrecoverable fraud losses.
- Will benefit from small increase in sales conversion due to frictionless, low latency payments for low risk, TRA-exempted transactions.

Scenario 2
Cost-benefit analysis of low-risk eligible transactions (50% of volume) flagged for TRA exemption:

- **Previous strategy:**
 100% of transactions sent for authentication; maximum fraud liability protection

- **New strategy:** Low-risk eligible transactions (50% of volume) flagged for TRA exemption; **increase in monthly sales between €1.5 million and €4.2 million***

*Retrospective analysis showed a potential increase of €1.5 million in March 2020 and of €4.2 million in May 2020

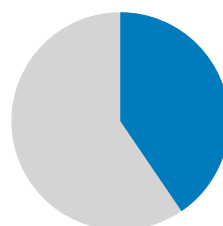


Take best advantage of the ways SCA can work for you

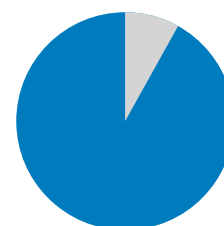
PSD2's requirement for SCA may have a significant impact for your customer's online payment journey and checkout experience.

Many regulatory authorities, including the UK's FCA, took a gradual ramp up approach to SCA enforcement, requiring a gradually increasing use of soft declines by issuers. As a result, many merchants were taken surprise by the impact of SCA, unable to handle issuers' soft declines or to ensure transactions were correctly flagged as exempt or out of scope. SCA enforcement forced many merchants to take swift action to ensure support for SCA for cardholder-initiated remote electronic transactions.

As issuers continued the SCA challenge ramp up in anticipation of the UK's 15th March 2022 SCA enforcement, one Elavon merchant customer experienced declines for 58% of transactions. Of those declined transactions, 90% were due to SCA being required.



● = % Transaction approved
1st - 8th Feb 2022



● = % Transaction approved
after applying Elavon TRA
exemption (from 10th Feb)

As the pie charts show, after enabling Elavon TRA the same customer's approval ratio achieved over 94% on average. This customer achieved 100% approval on some days, when all eligible transactions submitted with the TRA exemption request were approved by issuers.

Streamlined SCA processes and effective application of risk analysis and fraud management are key to optimising your online payments:

- Maximise application of SCA exemptions;
- Minimise disruption (frictionless transactions);
- Maximise conversion rates and business growth.

Talk to Elavon today to understand how leveraging the TRA exemption can help optimise payments for your business.

Take control by finding the right balance for your business between sales conversion, customer experience and fraud prevention.

Frequently asked questions

Frequently asked questions

A guide to Elavon's advanced fraud services and transaction risk analysis

- **What is transaction risk analysis?**

Transaction risk analysis (TRA) is an exemption from Secure Customer Authentication (SCA), which Elavon can offer. It means using a risk tool to flag low-risk transactions to Issuers. If they accept the exemption request, the transaction does not require SCA and that friction is removed. If the Issuer doesn't agree that the transaction is low risk, they can 'soft decline' it, or step it up, requiring the cardholder to authenticate themselves.

- **How does TRA work?**

There are two versions of TRA: Outsource TRA and Elavon TRA. For Outsource TRA, the merchant/gateway has their own risk tool that determines a transaction is low risk and flags the TRA exemption on a transaction request to Axis. Elavon TRA is where our advanced fraud service is used to assess the risk of a transaction. The TRA exemption can be requested on the authorisation request (Scenario 1 on page 25) or in the authentication request (Scenario 2 on page 26). In both cases, TRA can only be requested by Elavon for eCommerce transactions up to €500. This is based on Elavon's fraud reference rate.

- **What is Elavon's reference fraud rate?**

The amount up to which Elavon can apply TRA is determined by our reference fraud rate. This is calculated by the total value of unauthorised and fraudulent remote card

transactions divided by total value of all remote card transactions. Currently, this enables Elavon to allow transactions up to €500 to be exempted:

Transaction Value Band	Elavon Fraud Reference Rate
<€100	13 bps/0.13%
€100-€250	6bps/0.06%
€250-€500	1bps/0.01%

- **To which card types does it apply?**

TRA is only applicable for specific card schemes, namely Visa, Mastercard, Diners Club International, JCB and UnionPay International.

- **Does my payment service provider/gateway need to do any development or integration work for me to avail of Elavon TRA?**

Your payment service provider/gateway needs to support EMV 3-DS 2.x but Elavon does not require payment service provider/gateway certification.

- **I only want to avail of the Acquirer TRA exemption up to a transaction value that I specify (not Elavon's maximum €500 exemption threshold value), can I do that?**

Yes, you are able to ensure that transactions up to a value you choose are submitted for 3-DS authentication (no TRA exemption requested); while all transactions below that value can be flagged for TRA exemption.

- **Do I have to use 3-D Secure to get TRA?**

Merchants must support 3-D Secure on all eCommerce and mCommerce sales channels, as cardholders will need to use 3-D Secure to authenticate when a transaction is considered medium/high risk and so not approved for TRA. The card schemes will cease support for 3-DS 1.0.2 from 15 October 2022.

- **How do I get TRA?**

The Elavon fraud team will review your application but, as a general guideline, your processing volume should be greater than ten million transactions per annum, with an average transaction value <€500 and your fraud rate has been below 12 basis points for the past six months.

- **How much does it cost?**

This will be negotiated on a case-by-case basis. Bear in mind that Elavon incurs a fee from the card schemes every time an SCA exemption is requested.

- **What visibility will you give me of my online transactions?**

Amid concern PSD2 will see merchants lose control of how eCommerce orders are handled, Elavon advanced fraud services will help you gain more visibility of transactions declined due to suspected fraud, exemption requests (which orders were routed for acquirer exemption and which exemptions were granted by the Issuer), etc.

- **What expertise do you have in my industry and key markets?**

Elavon has a proven record of working with merchants of all scales and complexities across multiple markets, within North America, Europe – both inside and outside of the European Union – and cross-border. We work with multi-national franchises and global merchants to reduce fraud, improve revenue and performance for merchants in transportation, retail, hospitality and education, among many others. We help European based merchants (inside and outside the EU) minimise fraud risk for inbound cross-border transactions that are out of scope for SCA.

- **As fraud evolves, how will you be able to protect me against new fraud attack methods?**

Elavon's advanced fraud services will use advanced analytics and artificial intelligence that profile each customer's individual behaviour, use data elements specific to your business, including your transaction and fraud history, and an Elavon-wide holistic view of our entire global acquiring customer base to deliver dynamic risk analysis and real-time decision-making on your transactions. Our solution will learn from and adapt to changing customer behaviour, fraud patterns and attack methods.

- **How will you help my business maximise SCA exemptions?**

Elavon works with you to optimise your online payments and make sure your transactions include the relevant flags and indicators. Our solution focuses on maximising your revenue and minimising fraud. Our advanced fraud services analyse transactions prior to authentication and authorisation in order to filter out fraud attempts, maximise use of acquirer-requested exemptions (per your agreed preferences) and frictionless authentication, and reduce payment declines.

- **What technologies will feature in Elavon's advanced fraud services?**

Elavon advanced fraud services are a real-time transactional monitoring solution, which will have the capability to spot anomalies to block new fraud attacks and suspicious activity as it occurs. At the same time, the new Elavon fraud-detection system will be able to recognise genuine customers without blocking their activity, helping to improve acceptance rates while stopping fraud in its tracks. In addition to utilising the advantages of new fraud technologies/techniques – which have been developed to absorb and utilise known 'fraud features' – Elavon advanced fraud services will be able to spot changes in behaviour which could be an early indication of a fraud attack. Our wealth of knowledge and data across its whole portfolio enables you to take advantage of this new approach in the deployment of detecting and preventing fraud.

- **What data will Elavon's advanced fraud services draw on to ensure accuracy to reduce false positives and false negatives?**

The expertise of Elavon, gained through years of fraud-management knowledge, alongside the ongoing validation of fraudulent activity, ensures the delivery of immediate effective results and a solution that continually adapts and evolves, learning from the data ingested and monitored by the fraud-management solution in real time, 24/7.

- **What's your incentive to ensure my revenue remains protected under PSD2?**

Elavon wants to make sure all of our customers maximise their revenue, offer a low latency checkout experience to cardholders and minimise fraud. Making the right risk decisions (correctly blocking fraud) helps us to help you, reduces our risk where we take on the fraud liability and reduces the overall fraud rate of Elavon keeping our TRA Exemption Threshold Value as high as possible (currently €500, or equivalent local currency value).

- **Can my company's internal and external data sources be used to enrich the gathered data used in the advanced fraud services data model and risk analysis?**

Elavon will utilise each and every data element it has at its disposal to ensure the new fraud system is learning from the most current and up-to-date information. When new data elements become available, these will be assessed and, where applicable, introduced to ensure the fraud solution remains future proofed.

-
- **How does Elavon's advanced fraud services scale and adapt to a changing fraud environment?**

The new fraud system being deployed by Elavon has been designed to continually evolve, learning from changing patterns across our whole portfolio. This fraud model will assign each merchant to a consortia or peer group, ensuring every transaction, regardless of whether it's the very first transaction, is assessed against historic data to ensure it is in line with what is expected for that particular type of business. The model will be continually provided with new information to ensure it is operating on the most current information available.

- **How do Elavon's advanced fraud services leverage artificial intelligence/machine learning to proactively detect fraud patterns and block fraudulent transactions?**

Elavon advanced fraud services will incorporate a vast amount of information across our whole portfolio, ensuring the most up-to-date information is available, alongside confirmed fraud. By utilising Featurespace's already proven advanced analytics and artificial intelligence technology, our advanced fraud services will be highly effective in identifying more fraudulent transactions than a 'rules based' fraud system, which needs constant monitoring and ultimately leads to reactive fraud management rather than proactive fraud management. Additionally, Elavon recognises that fraud constantly evolves in order to avoid detection. It is for this reason, we have introduced this new approach, leveraging market leading technology to protect our customers.

-
- **Can Elavon's advanced fraud services help improve my operational efficiency?**

Elavon advanced fraud services offer automation of previously onerous, manual processes and the ability to customise workflows. Elavon recognises the resource demands and cost reduction pressures on all businesses, regardless of size, why we are developing and introducing this new solution to help limit the potential operational overhead associated with fraud monitoring and management.

- **How can Elavon's advanced fraud services protect my business from account takeover?**

Account takeover is where fraudsters gain access to legitimate customer's credentials – usually as a result of a data breach – and use them to order goods.

See box below

- **Can Elavon's advanced fraud services protect my business from automated 'bot' fraud attacks?**

Carding or card cracking are forms of automated 'bot' attacks. Fraudsters use these techniques to test stolen card

data by carrying out multiple payment authorisation attempts to identify valid card details (carding) or to identify missing elements of stolen payment card information (card cracking).

See box below

- **How do Elavon's advanced fraud services protect my business from 'friendly fraud'?**

'Friendly fraud' is when a cardholder makes an online shopping purchase with their own credit card, and then requests a chargeback after receiving the purchased goods or services disputing that it was actually them that made the purchase.

See box below

The Elavon advanced fraud services approach is the same (albeit with some variation specific to the fraud type) for each of these types of fraud attack above.


Through the review and understanding of fraudulent behaviour from the past, Elavon has designed our advanced fraud services to incorporate a model that has capability to track and identify what 'good' looks like, through the review and understanding of fraudulent behaviour from the past; by default the 'bad' (or fraudulent) transactions will fall out.

This is a different approach to other fraud solutions which are modelled/created based on fraudulent transactions and as a consequence

have to wait for the fraud to happen and be reported for the fraud system to be updated so that the fraud can be detected.

The new approach by Elavon advanced fraud services will identify changes in behaviour that could indicate a potential fraud not seen before. Elavon advanced fraud services will be capable of identifying this behavioural change, whereas other fraud systems can only react after the fraud has occurred.

For frequently asked questions about PSD2, please [click here](#).

A white rectangular box is positioned in the lower right quadrant of the page, partially overlapping a horizontal white line that spans the width of the page.

Elavon Financial Services DAC. Registered in Ireland – Number 418442.
Registered Office: Block F1, Cherrywood Business Park, Dublin 18, D18 W2X7, Ireland
Elavon Financial Services DAC, trading as Elavon Merchant Services, is regulated by the Central Bank of Ireland.

Elavon Financial Services DAC. Registered in Ireland with Companies Registration Office. The liability of the member is limited. United Kingdom branch registered in England and Wales under the number BR022122.
Elavon Financial Services DAC, trading as Elavon Merchant Services, is deemed authorised and regulated by the Financial Conduct Authority. Details of the Temporary Permissions Regime, which allows EEA-based firms to operate in the UK for a limited period while seeking full authorisation, are available on the Financial Conduct Authority's website.