Payments Optimisation

Maximise conversion, minimise fraud

Elavon

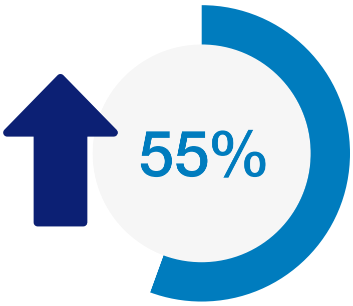
Take control: optimise your online payments

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

Online payments are a prime target for fraudsters. European card fraud reached

€1.55bn in 2019.

Remote-purchase fraud represents more than three quarters (76%) of this, linked to the increasing use of cards for online payments. Fraud has continued to increase and has risen by since the beginning of the COVID-19 pandemic in early 2020. 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.

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.

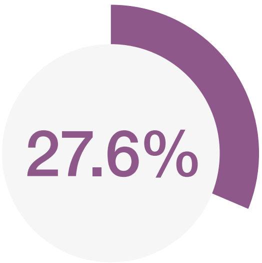
Our payments optimisation insight will help you streamline the shopper checkout experience, to maximise sales while minimising your fraud risk. This white paper explores the opportunities offered by SCA – and its exemptions – and examines ways to minimise its impacts on your business and customers.

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.

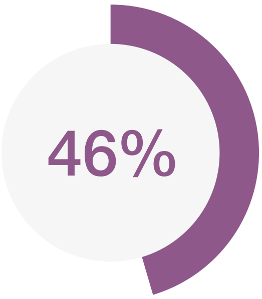
Contents

The growth of online shopping and increases in eCommerce fraud

Tens of thousands of merchants enter the online market each year. It is estimated that in 2020, worldwide retail eCommerce sales grew by 27.6% even as total worldwide retail sales declined by 3.0%.



In some countries, online sales growth in 2020 was even greater: UK eCommerce grew by 46%, its strongest growth in more than a decade.



The growth of online commerce as a percentage of total retail sales is striking. In the US, eCommerce now accounts for 21.3% of total retail sales, up nearly 5% in one year.

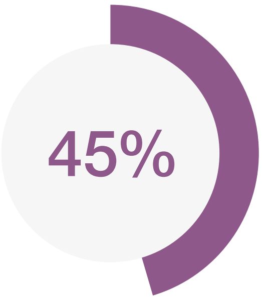
In the UK, the changing ratio is even more pronounced. As of January 2021, internet sales accounted for 36.3% of total retail sales, representing a 22.1% shift online in five years. There has also been a shift from desktop to mobile: in 2020, some 67% of all online transactions were carried out on mobile devices, largely (72%) 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.

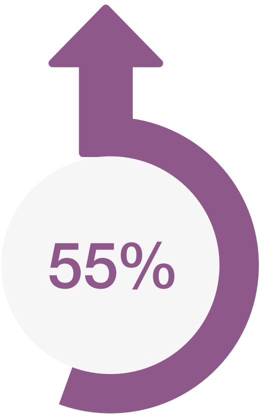
Recent research has indicated that in 2019, card fraud across Europe had reached

€1.55bn.

The UK accounted for almost half (45%) of that, and more than three quarters (76%) of this fraud happened during remote purchases, where an electronic payment is made 'at a distance' and neither card nor customer are physically present (such as an eCommerce or mobile payment).



Rates of fraud have continued to increase through 2020, with pymnts.com reporting a fraud-rate increase of 55% since the beginning of the COVID-19 pandemic.



Globally, financial loss caused by payment fraud tripled from

$9.84bn

in 2011

$32.39bn

in 2020.

By 2024, online payment fraud is expected to cost eCommerce merchants more than $25 billion annually.[1] Other researchers, looking further ahead, predict that global losses in 2027 for all payment fraud[2] will be

25%

higher than in 2020 ($40.62 billion). 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 2020 True Cost of Fraud Study, LexisNexis Risk Solutions found that US online retail merchants incurred

$3.36

costs for every

$1

of fraud committed, compared to $3.13 in 2019.

Cybercriminals and even casual fraudsters give eCommerce extra attention during peak periods – such as the festive season and other holidays – when they know merchants are typically overwhelmed with orders.

[1] Juniper Research, Online Payment Fraud: Emerging Threats, Segment Analysis & Market Forecasts 2020-2024 report

[2] Global fraud losses incurred by payment card issuers, merchants, acquirers of card transactions from merchants, and acquirers of card transactions at ATMs on all credit, debit and prepaid general purpose and private-label payment cards worldwide.

Many online businesses have also seen a huge surge in eCommerce purchases, as stores closed due to the stay-at-home directives during the COVID-19 pandemic:

- Globally, the increase in retail website traffic surpassed holiday season peaks: up from 16 billion global visits in January 2020 to almost 22 billion visits in June 2020, according to Statista.
- Online sales in the UK alone showed record growth during May 2020: some 129.5% even as total worldwide retail sales declined by 3.0%.
- In Italy, eCommerce sales for consumer products rose by 81% in a single week in March 2020.[3]
- Even after the initial growth peak, studies showed a 38% year-on-year increase in global eCommerce transaction volume for the second half of 2020.

As with holiday peak periods, the increase in online sales saw a rise in eCommerce fraud attempts, with online retail a primary target. Payments Cards & Mobile reported on one COVID-19 eCommerce fraud tracker, which showed the attempted payment fraud rate had increased by

50%

in the first quarter of 2020. While LexisNexis noted that growth in fraud has not been recorded across all digital businesses, it is fair to say that in uncertain times, it can be even harder to identify fraudulent activity.

During such times of dramatic change in consumer behaviour, what they buy, when they buy it and where they buy it from evolves, rapidly. That same tracker showed fraud rates for ‘buy online, pick up in-store’ (BOPIS or ‘click and collect’) purchases up by

68%

as social distancing and stay-at-home orders impacted consumer behaviour.

[3] GDOWeek: March 6, 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.

While also:

- Maximising sales opportunities
- Limiting the impact on your customer experience
- Increasing conversion rates.

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.

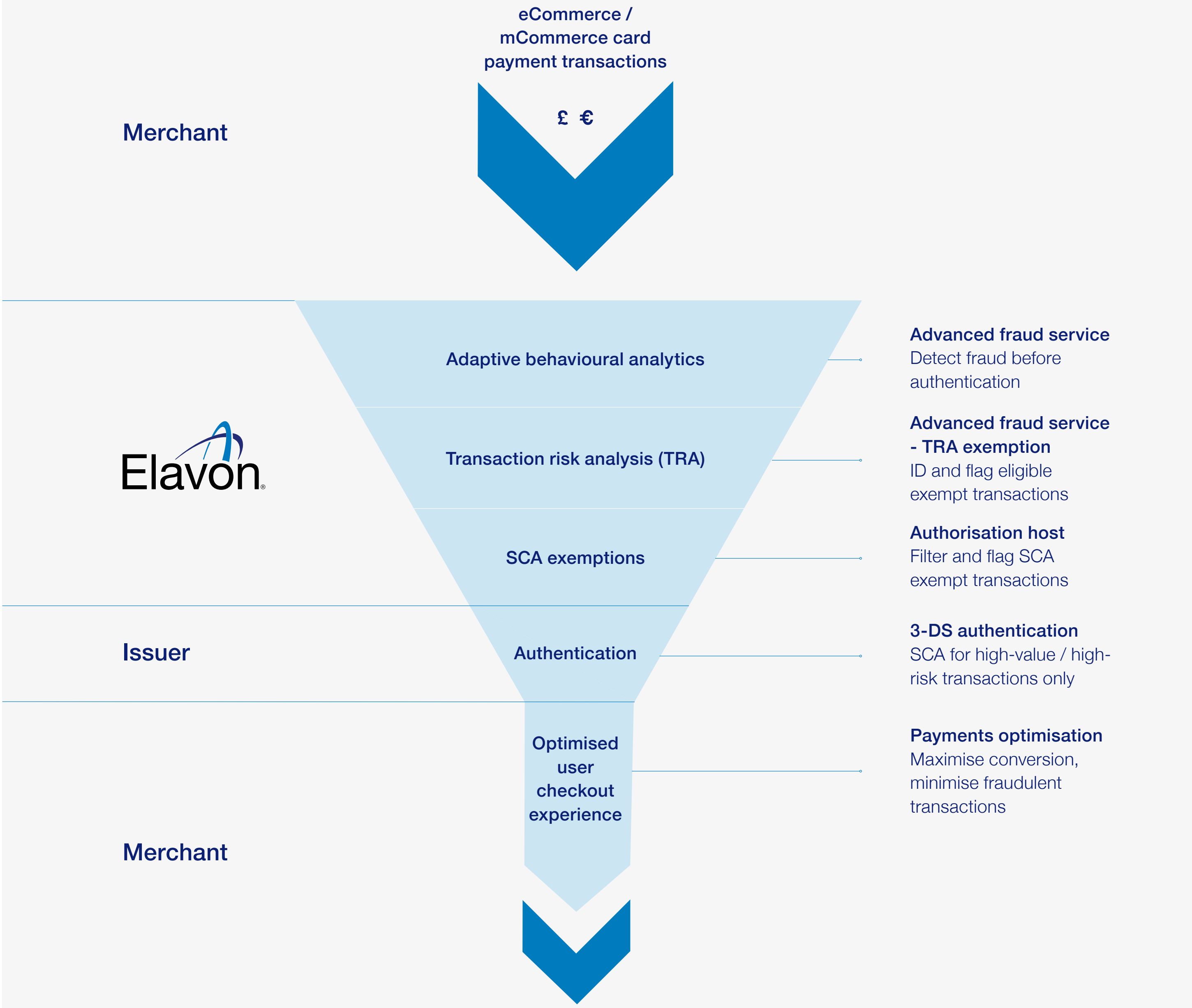
The advanced fraud services at Elavon will serve to protect your customers and your business from fraudulent transactions by making best use of bespoke data-science models: **machine learning** and **adaptive behavioural analytics.**

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 machine learning and adaptive behavioural analytics 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', p10).*
- For quicker transaction times that streamline your customers' checkout experience, maximising shopping cart conversion and increasing online sales.


eCommerce / mCommerce card payment transactions
£ €
Merchant
Adaptive behavioural analytics
Transaction risk analysis (TRA)
SCA exemptions
Elavon
Issuer
Authentication
Optimised user checkout experience
Merchant

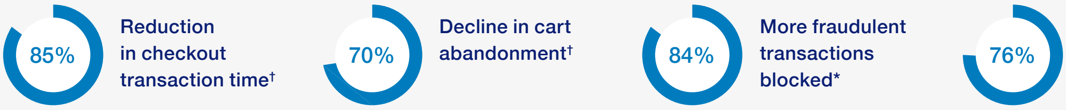
Advanced fraud service
Detect fraud before authentication

Advanced fraud service - TRA exemption
ID and flag eligible exempt transactions

Authorisation host
Filter and flag SCA exempt transactions

3-DS authentication
SCA for high-value / high-risk transactions only

Payments optimisation
Maximise conversion, minimise fraudulent transactions



85% Reduction in checkout transaction time[†]

70% Decline in cart abandonment[†]

84% More fraudulent transactions blocked*

76% Fewer genuine transactions declined*

*taken from 'PSD2 & Strong Customer Authentication: What Acquirers Need to Know': www.featurespace.com/resources/psd2-guide-to-sca-for-acquirers/
†based on Visa risk-based authentication case study "Frictionless Experience with Verified by Visa,": https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-3-D-secure-2-program-infographic.pdf

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 aims to:

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

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

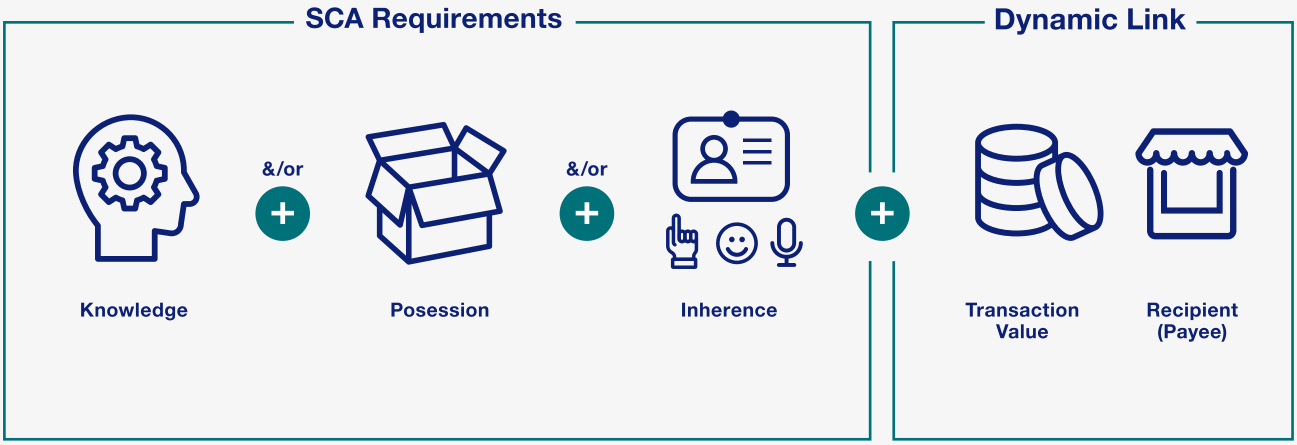
Enforcement of SCA for all transactions in scope is the final step in implementation of the technical measures needed to achieve PSD2's aims.

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':



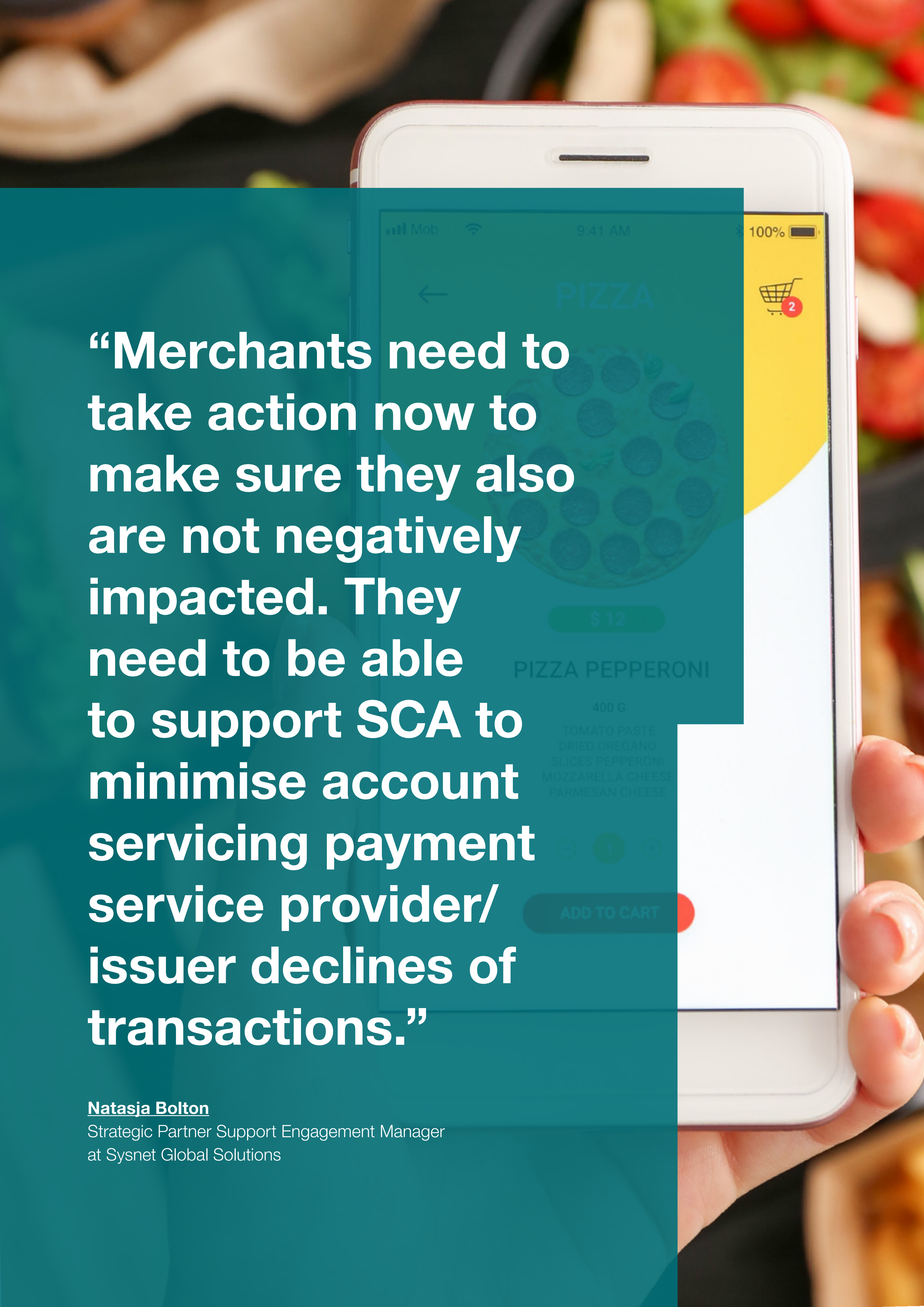
The enforcement date for SCA was from 14 September 2019. However, significant concerns about the state of readiness of the payments industry, the potential impact on payments and the risk of negative consequences for cardholders led to the European Banking Authority (EBA) postponing enforcement of SCA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

Location of card issuer	SCA enforcement deadline
EEA countries[4] excluding UK	31 December 2020
United Kingdom	14 March 2022

With the SCA enforcement deadline now passed for 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). However, online retailers have not been experiencing a Europe-wide mass decline of transactions as the EEA enforcement deadline passed.

This is because SCA compliance is the responsibility of individual countries' national competent authorities (NCAs). Some NCAs, such as Banque de France and Central Bank of Ireland, had already set a later implementation date and gradual migration to full enforcement. Many others, such as Germany's Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), had set out a timeline for a gradual ramp-up through the use of soft declines for non-compliant transactions above certain value thresholds. Yet other NCAs (such as Banco De Portugal) have not enforced at all, even without extended deadlines or agreed ramp-up periods. That Europe has not seen a mass decline of transactions is largely due to these NCAs gradually ramping up to full SCA compliance. Merchants need to take advantage of this limited period of flexibility, or 'soft enforcement', to understand how SCA may impact their online payments and prepare for subsequent stricter enforcement of SCA.

[4] EEA countries are all 27 EU member states plus Iceland, Liechtenstein and Norway.



“Merchants need to take action now to make sure they also are not negatively impacted. They need to be able to support SCA to minimise account servicing payment service provider/ issuer declines of transactions.”

Natasja Bolton
Strategic Partner Support Engagement Manager
at Sysnet Global Solutions

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.

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

Recent Microsoft testing showed low rates of success for SCA challenge authentication with customers unable to complete their transaction.

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".*

As card issuers are required to apply SCA, it will therefore be 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.

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 be able 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 be ready 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 [p16]).

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

<table>
<tr><th colspan="2">In scope for SCA</th><th rowspan="2">Out of scope</th></tr>
<tr><th colspan="2">Available SCA exemptions</th></tr>
<tr><td><b>Acquirer PSPs</b></td><td><b>Issuer PSPs</b></td><td rowspan="6"><b>Unattended</b> transport fares and parking fees
<b>Anonymous pre-paid</b> transactions
Payments initiated by <b>mail or telephone (MOTO)</b>
<b>‘One-leg out’</b> transactions[5]
<b>‘One-leg in’</b> transactions[6]
Merchant initiated transactions <b>(MITs)</b>[7]</td></tr>
<tr><td colspan="2"><b>Low-value remote electronic payment transactions</b>
Payments €30 or below; issuer counter limit:
€100 cumulative spend or five consecutive transactions</td></tr>
<tr><td colspan="2"><b>Recurring transactions</b>
of the same amount and to the same merchant</td></tr>
<tr><td colspan="2"><b>Transaction risk analysis (TRA)</b>
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</td></tr>
<tr><td></td><td>Payments to <b>trusted beneficiaries</b></td></tr>
<tr><td></td><td><b>Secure corporate payments</b></td></tr>
</table>

[5] 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.
[6] One-leg in: the cardholder’s PSP (the Issuer) is located outside the EEA or UK; the issuer is not subject to PSD2
[7] 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 choice[8]. 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’).

[8] Visa PSD2 SCA Optimisation Best Practice Guide v1.0, July 2020

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)	€500	€250	€100
Acquirer fraud rate	<= 0.01%	<= 0.06%	<= 0.13%

The reference fraud rate at Elavon is currently less than 0.06%, allowing us to apply TRA exemption for customer transactions up to €250 (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 [p16], as and when SCA is required)

Enforcement of SCA in some European countries is not yet fully applied, with some SCA deadline dates still to be reached and many NCAs supporting a gradual ramp-up. However, to be ready for the 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;
- Update business processes and systems to ensure SCA is supported 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.

- Optimise the integration of 3-D Secure SCA challenge screens into browser and app checkout;
- Ensure all required 3-D Secure data points are available for issuer evaluation to support accurate decision-making;
- 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	Merchants wishing to leverage acquirer TRA exemption for eligible transactions below Elavon ETV, (see p19) *and* Willing to make own decision on taking on transaction fraud liability.	Merchants wishing to leverage the Elavon risk engine to seek SCA exemption for eligible transactions. Merchants willing to accept Elavon's decision on taking on transaction fraud liability.
Eligibility	Merchants with existing risk analysis and fraud management capability.[9] Able to support 3-D Secure 2 and respond to soft declines. Fraud rate for most recent six months is less than 12bps (0.12%). Technical capability to include TRA exemption indicator in the authorisation request.	Able to support 3-D Secure 2 and respond to soft declines. Average transaction value up to €250. Fraud rate for most recent six months is less than 12bps (0.12%). Technical capability to include TRA exemption indicator in the authorisation request.

[9] 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.

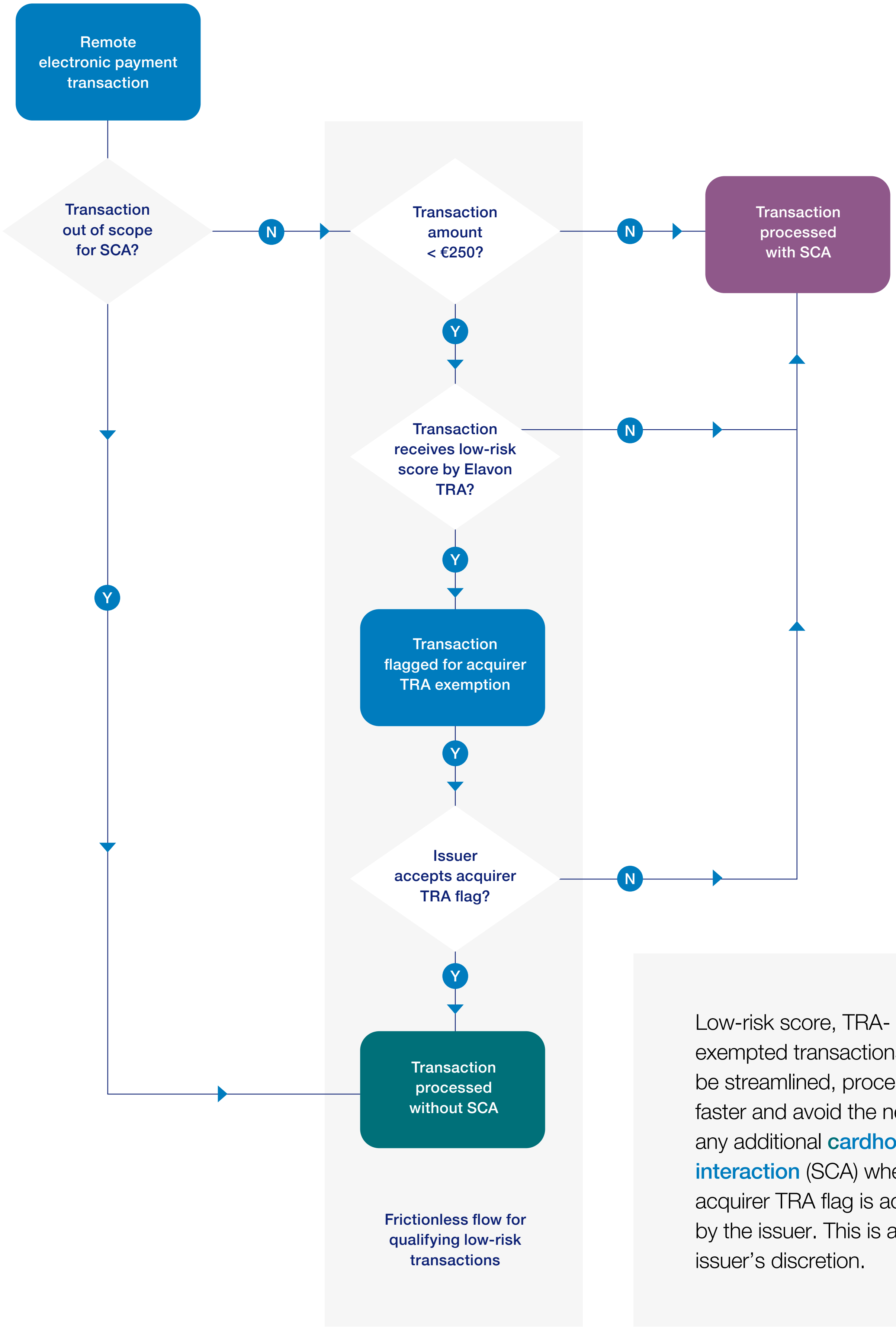
Elavon TRA is performed in real-time with an instant response. This saving in transaction latency is another reason eligible customers are encouraged to sign-up for Elavon TRA. Cardholders will experience a frictionless checkout for low-risk score, TRA-exempted transactions that are sent straight to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


Remote electronic payment transaction
Transaction out of scope for SCA?
N
Y
Transaction amount < €250?
N
Y
Transaction processed with SCA
Transaction receives low-risk score by Elavon TRA?
N
Y
Transaction flagged for acquirer TRA exemption
Y
Issuer accepts acquirer TRA flag?
N
Y
Transaction processed without SCA
Frictionless flow for qualifying low-risk transactions

Low-risk score, TRA-exempted transactions may be streamlined, processed faster and avoid the need for any additional **cardholder interaction** (SCA) when the acquirer TRA flag is accepted by the issuer. This is at the issuer's discretion.

Elavon TRA – detailed scenarios and their benefits

Scenario 1:

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

For eligible transactions ≤€250 (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').

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, in this scenario, the cardholder must be available for SCA if step-up is requested.

Scenario 2:

Transaction **submitted for authentication** (via 3-D Secure) flagged with the acquirer TRA exemption flag and then **submitted for authorisation**.

For transactions where authorisation may be delayed, as the cardholder will still be available to authenticate if SCA challenge is required.

Payment may be **authenticated frictionless,** without a step-up challenge.

Potential to offer lower transaction latency/ processing time.

Issuers may have a preference for this route; approval rates may be higher.

In this scenario, issuers carry out their own risk assessment based on the available authentication data.

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, and the transaction value is within the issuer's own ETV, 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, or the transaction value is outside the issuer's ETV, will an SCA challenge be triggered.

In both cases, fraud liability is with you (the merchant).

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.[10] 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.

[10] Mastercard PSD2 RTS Readiness Status and Heightened Awareness Update, 29 January 2021

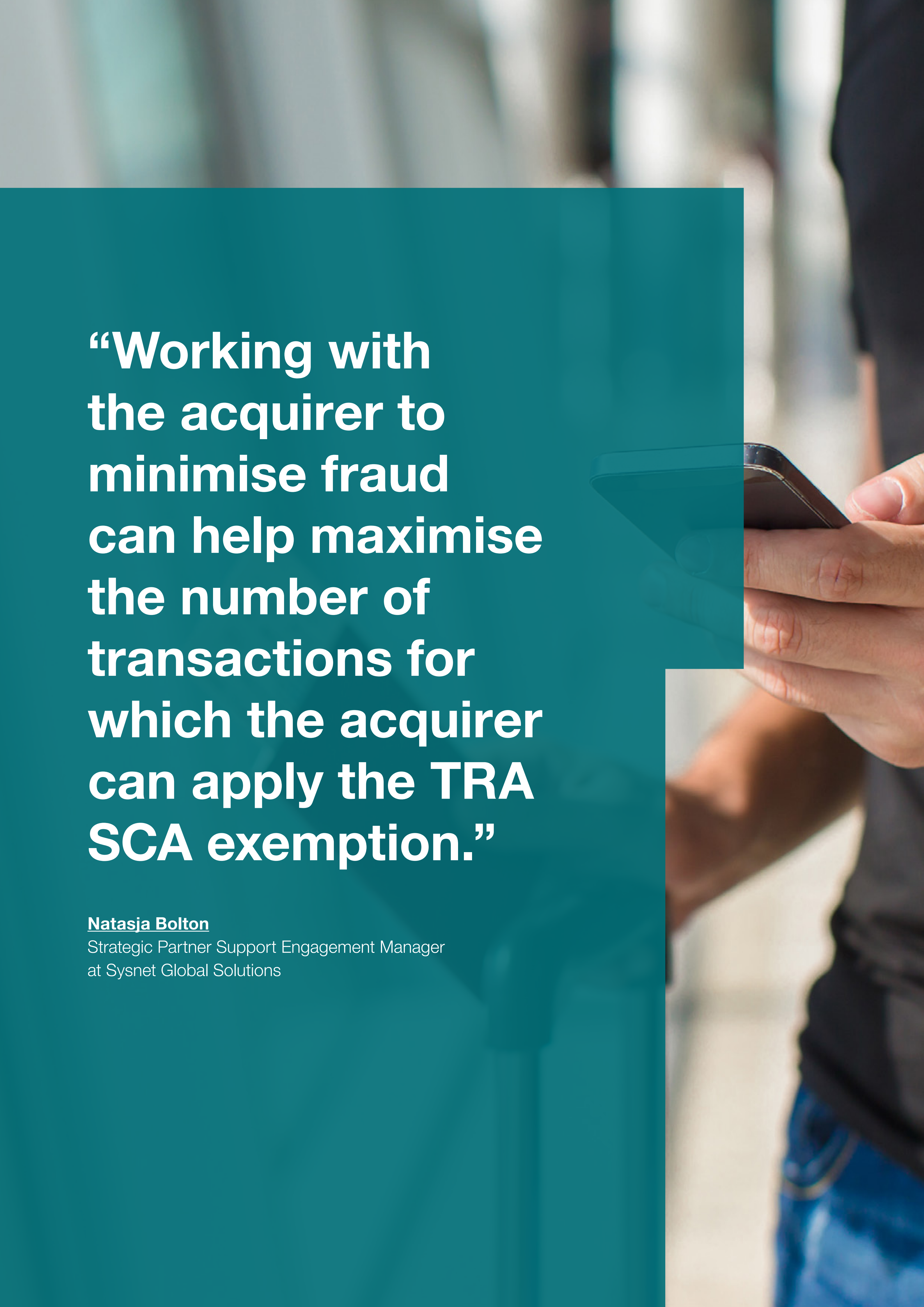
Impact of SCA for Elavon customers operating outside Europe

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:

	Location of:		
In scope/ out of scope	**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.



“Working with the acquirer to minimise fraud can help maximise the number of transactions for which the acquirer can apply the TRA SCA exemption.”

Natasja Bolton
Strategic Partner Support Engagement Manager
at Sysnet Global Solutions

Key factors in minimising SCA on customer transactions

Minimise fraud

Work to minimise misreported and 'friendly' fraud[11] 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 status[12].

[11] 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.
[12] 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.

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.

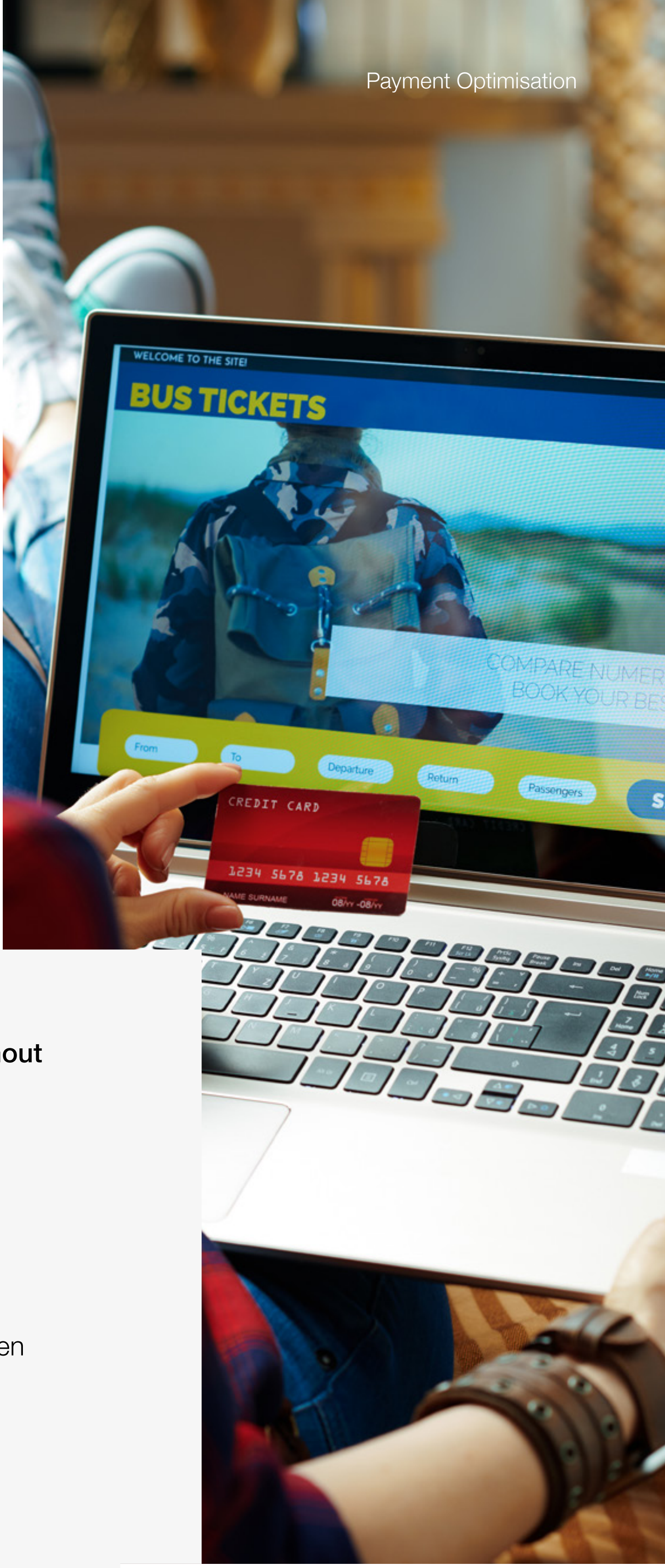
The main implication of applying an SCA exemption is that Elavon (and hence you, our customer) takes on the liability for the transaction and any subsequent fraud.

Why request the TRA exemption?

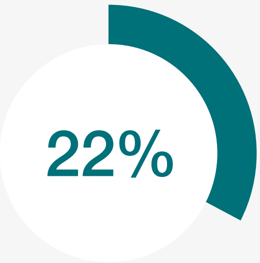
Simply put, Elavon TRA can help you find your ‘sweet spot’ to achieve payments optimisation.

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.**

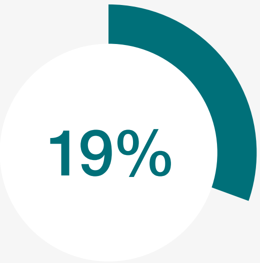
Payments optimisation is about balancing the desire to maximise conversion and increase sales with the need to avoid chargebacks and fraud losses.



Potential impact of SCA without payments optimisation



22% of payments sent for 3-D Secure authentication are lost. This loss could be due to low acceptance rates, but also increased latency (the time taken to authenticate and complete 3-DS), leading to consumer frustration and drop off.



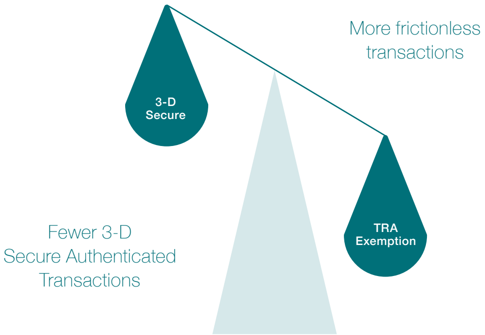
19% of payments were still lost, even with the improved 3-D Secure 2 consumer experience.

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

Finding your balance

With low risk, low average transaction value and low fraud rate, you will be able to:

- ⬆ Maximise use of TRA exemption and
- ⬇ Minimise the number of transactions requiring SCA.


More frictionless transactions
3-D Secure
TRA Exemption
Fewer 3-D Secure Authenticated Transactions

By using Elavon TRA, all 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.

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:

- All eligible, low-risk transactions below Elavon ETV 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:

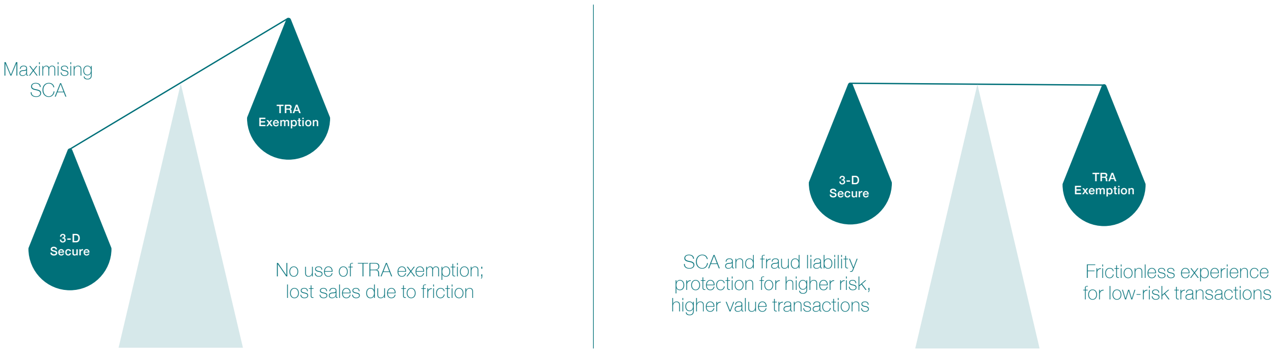
- Higher value, higher-risk transactions will be submitted for authentication, giving the merchant fraud liability protection and minimising unrecoverable fraud losses.
- Will benefit from small increase in sales/ conversion due to frictionless, low latency payments for low risk, TRA-exempted transactions.

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


Maximising SCA
TRA Exemption
3-D Secure
No use of TRA exemption; lost sales due to friction
3-D Secure
TRA Exemption
SCA and fraud liability protection for higher risk, higher value transactions
Frictionless experience for low-risk transactions

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.

While the active enforcement of SCA has been rolling out at different dates across the EEA, the final implications are that all merchants must be able to support SCA for cardholder-initiated remote electronic transactions.

Although many regulatory authorities have taken a gradual ramp-up approach post-enforcement through the use of soft declines, merchants will find that those transactions that are not out of scope or flagged as exempt, will be impacted and may be declined by issuers. Merchants should also note that some issuing banks enforce SCA ahead of the deadlines, declining some payments that are not ready for SCA.

Streamlined SCA processes and effective application of risk analysis and fraud management will be 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.

Elavon Financial Services DAC. Registered in Ireland – Number 418442. Registered Office: Building 8, Cherrywood Business Park, Loughlinstown, Co. Dublin, D18 W319, 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 authorised and regulated by the Central Bank of Ireland. Authorised by the Prudential Regulation Authority and with deemed variation of permission. Subject to regulation by the Financial Conduct Authority and limited regulation by the Prudential Regulation 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.

Elavon®