Cybersource+ Insights

Strong Customer Authentication (SCA)

How to manage out-of-scope transactions and optimize exemption strategies

cybersource
A Visa Solution

Contents

About this guide

The shift to digital shopping has been significant during the pandemic: years of changes in consumer behavior were compressed into a matter of months. Across multiple markets, there was rapid growth in the number of consumers that started their purchase on digital channels.

Nearly two years into their own digital transformations, a new, more mobile consumer is now using mobile devices more to shop and pay. In a recent PYMNTS and Cybersource survey, over forty percent of consumers in the nations studied used smartphones at least one point during their recent shopping journeys in 2021[1] – whether to purchase products on their phones, compare prices online, pay at a brick-and-mortar POS, or something else.

At the same time, the entire payments ecosystem has been preparing in earnest for the introduction of PSD2 SCA, which has been fully enforced since January 2021 across a number of European markets, and from mid March 2022 in the UK.

[1] The 2022 Global Digital Shopping Index, Cybersource and PYMNTS, February 2022. Nations studied: Australia, Brazil, UAE, U.K., U.S. and Mexico

Mari-anne Bayliss
Senior Director, Solutions Management
Cybersource

Mari-anne is Cybersource's PSD2 SCA expert. She partners with clients to develop solutions that provide great customer experiences, and keep their business secure.

Prior to this, Mari-anne spent 18 years with a large U.K. retailer, leading the eCommerce fraud and internal risk management teams. With this experience, she brings a unique perspective on today's digital payment landscape.

[1] The Global Digital Shopping Index reports, Cybersource and PYMNTS, 2020

Of course, wherever there's change, there's opportunity. Successful, forward-looking brands are taking the opportunity to redefine and reimagine the digital consumer experience, and make it the best it can be.

A big part of that is providing the convenient, secure and frictionless eCommerce payment experiences customers expect. So it's critical for merchants to deal well with enforcement of PSD2 Strong Customer Authentication (SCA) requirements. This means supporting the mandate while keeping the customer experience seamless, and minimizing the chance of cart abandonment.

This guide is designed to help merchants who may be required to support the PSD2 SCA mandate make a smooth transition to SCA, and help maintain a great payment experience for customers.

You'll learn some best practice approaches to:

1. **Deliver an optimal experience for customers when SCA challenges are required (i.e. when a consumer is asked to go through an authentication process).**
2. **Minimize the need for SCA challenges through effective management of transactions that are out of scope for, or may be exempt from, SCA.**

What is SCA and when does it apply?

Under PSD2, Strong Customer Authentication (SCA) must be applied to electronic payments within the European Economic Area (EEA) and the U.K., unless:

- The payment is out of scope for SCA; or
- An exemption to SCA applies

SCA requires the payer to be authenticated by two or more of the following:

- **Inherence:** Something the payer is, such as fingerprint or voice recognition (biometrics)
- **Possession:** Something only the payer has, such as a pre-registered mobile device, card reader or key generation device
- **Knowledge:** Something the payer knows, such as a PIN or password

Some European markets implemented full SCA enforcement on 1 January 2021; others phased it in over the course of the year. For U.K. and Ireland enforcement was in March 2022.

For more comprehensive PSD2 SCA resources, visit the Visa website.

Make a smoother transition to SCA

The following best practice guidance is designed to help you make a smooth transition to SCA and maintain a great payment experience for your customers.

It outlines two key areas for merchants to focus on, and where Cybersource can help:

1. Minimizing friction when SCA challenges are required (an SCA challenge is when a consumer is asked to go through the authentication process).

2. Minimizing the need for SCA challenges by identifying transactions that are out of scope, or may be exempt.

Minimize friction for customers when SCA is required

When implemented well, SCA doesn't generally impact on the customer payment experience. The EEA rollout proved relatively painless, and shows that:

- Exemptions are generally being applied by acquirers and issuers
- The volume of transactions requiring authentication appears to be lower than anticipated

According to Visa, European eCommerce approval rates are tracking at 95% (excluding declines due to insufficient funds), which "suggests that Europe has successfully implemented SCA in a way that avoids major disruption."[2]

To minimize the impact of SCA on the checkout experience, merchants need to make the SCA challenge process as smooth as possible.

You can do this by using the latest version of the 3-D Secure protocol —EMV® 3DS—which provides for smoother payment authentication on the devices consumers shop from today, such as mobiles.

[2] "The Long and Winding Road to SCA," The Payments Association, December 2021

The Cybersource Payer Authentication solution incorporates all the features and benefits of EMV® 3DS. You can use Payer Authentication to provide customers with:

- An optimized SCA experience that's integrated with the shopping experience and works seamlessly on any device
- Smarter and broader authentication options, including one-time passwords (OTPs), biometric identification, and out-of-band authentication
- Authentication that extends to in-app purchases and digital wallets

And because EMV® 3DS allows up to 10 times more data to be shared, issuers will have richer information on which to base more accurate fraud risk assessments, which can lead to higher authorization rates.

Take action

If you're not yet using EMV® 3DS (the latest version of 3-D Secure), consider upgrading so that you can benefit from exemptions and offer customers the best authentication experience available. Please note 3DS 1 is being sunset in October 2022. Merchants who continue using 3DS 1 after the sunset date may be liable for fraud on some transactions, even if authenticated. Check your liability position with your acquirer or payment gateway.

Minimize the need for SCA challenges

SCA doesn't apply to all transactions: some transactions are out of scope for SCA, and others may be exempted from authentication.

To minimize friction for your customers by performing SCA only when it's needed, you need to be able to do two things:

1 Correctly identify out-of-scope transactions

2 Request exemptions for qualifying transactions

Minimize the need for SCA challenges

(continued from previous page)

Manage out-of-scope transactions

Merchants must be able to identify and flag the following out-of-scope transaction types.

Mail order/telephone order (MOTO)

Transactions where payment is taken by mail order or over the phone are out of scope for SCA. Merchants must be able to flag MOTO transactions correctly so that issuers don't decline them for SCA.

One leg out (OLO)

It may not be possible to apply SCA to a transaction where either the issuer or acquirer is located outside the EEA or the U.K.[3] However, SCA should still be applied to OLO transactions on a "best efforts basis". The issuer should make its own approval decision based on risk and liability considerations.

- In the case where a transaction uses a card issued in the EEA or the U.K., but is acquired outside the EEA or the U.K., the issuer should decide whether to approve, challenge or decline the transaction based on their risk assessment, the liability implications and the impact on the consumer experience. If the issuer is not technically able to impose SCA, the issuer is not obliged to decline.
- In the case where a transaction uses a card issued outside the EEA or the U.K., but is acquired within the EEA or the U.K., it is recommended that acquirers/merchants send transactions in an SCA compliant way, such as via 3-D Secure, where the issuer supports this. The issuer is not obliged to apply SCA.

It should be noted that a transaction at a merchant that is located outside the EEA or U.K. but that is acquired from within the EEA or U.K. is not classed as one-leg-out and is in scope of SCA.[4]

Merchant Initiated Transactions (MITs)

A series of transactions for fixed or variable amounts, such as subscriptions, are generally out of scope. SCA should be applied to the first transaction in the series. The next section tells you more about MITs.

[3] With SCA now fully enforced, SCA should be applied by all parties for U.K. and EEA cross border transactions.
[4] These transactions are identifiable by the issuer BIN or the acquirer location being outside the EEA or the U.K.

More about MITs

SCA must be applied to the first transaction in the series, when the customer is available to initiate or authenticate the payment. You or your payment gateway will need to store the transaction ID from this initial set-up transaction (or, in some cases, from a previous MIT).

You can then initiate subsequent payment requests without the direct involvement of the cardholder. To prevent these transactions being declined for SCA by issuers, you should flag them as out of scope by including the following information with each MIT authorization request you submit:

- The stored transaction ID
- The indicator identifying the MIT type

MITs may also arise when the final value of a transaction is higher than the amount presented during authentication.

For example:

- A hotel room booking, where extra costs like breakfast increase the total
- A hire car is returned without refueling, and the rental company then charges for the refill
- Video services with paid add-ons, such as pay-per-view movies, that increase the monthly bill total

Minimize the need for SCA challenges

(continued from previous page)

To comply with the 'dynamic linking' aspect of these transactions and help make checkout more frictionless, merchants should adopt a mitigation strategy. One option may be to use MIT incremental authorizations for additional unauthenticated amounts, rather than adjusting the final or monthly payment, as long as the final amount is within the terms and conditions agreed upon with the cardholder at mandate setup.

Guidelines vary from scheme to scheme, so check with your payment gateway or acquirer to understand the best approach.

Your checklist for handling out-of-scope transactions:

1 **Check how your acquirer or payment gateway would like you to identify MITs and other out-of-scope transactions. They'll advise you on the framework to follow.**

- Bear in mind that some acquirers use a proprietary standard for flags, which they convert to the appropriate card scheme standard before submitting an authorization request

2 **Speak to your payment gateway or acquirer as soon as possible to agree:**

- Which types of out-of-scope transaction they're processing (if any)
- How out-of-scope transactions should be identified and flagged
- For MITs:
  - How the set-up of an MIT agreement should be authenticated
  - How initial or prior transaction IDs should be captured, stored and populated into authorization requests

Minimize the need for SCA challenges (continued from previous page)

Optimize your exemption strategy

Some types of transaction that are in scope for SCA may be exempted from authentication. Only acquirers and issuers can apply the transaction risk analysis (TRA) exemption to transactions that would otherwise require SCA. Merchants must request the TRA exemption from their acquirers. The issuer always makes the ultimate decision on whether or not to accept or apply an exemption and may wish to apply SCA or decline the transaction.

Key exemptions

The following transaction types are, or can be, exempted from SCA. Merchants using 3DS 1 can't ask for exemptions.

Low value

If the transaction value is below €30 / £25, it won't require SCA. Merchants don't need acquirer approval to use the 'low value' exemption. These transactions can go straight to authorization. But the issuer will overrule this exemption once a card:

- Accumulates five transactions without a challenge for SCA (so the sixth transaction will be challenged); or
- Reaches a cumulative value of more than €100 / £85 without an SCA challenge (a challenge for SCA will reset the card's counter to zero)

Low risk (TRA exemption)

Merchants must gain agreement from their acquirers for TRA exemptions. The TRA exemption can be requested in authentication or authorization. After carrying out transaction risk analysis (TRA), the acquirer or issuer decides that the transaction is low risk and doesn't need to be challenged for SCA. TRA may be applied to transactions up to €500 / £440, but some issuers' upper limit may be lower.

Trusted beneficiary

If a customer's bank or card issuer supports trusted beneficiaries, a paying customer may be able to add merchants to a personal list of trusted beneficiaries (also known as 'trusted listing' or 'whitelisting'). After authentication of the first transaction with a merchant on the list, subsequent transactions may then be exempt from SCA.

Minimize the need for SCA challenges

(continued from previous page)

Influence SCA exemptions

Merchants who want to develop an SCA exemption strategy should consult with their payment gateway and acquirer.

The recommended starting point for your strategy—which you must pre-agree with your acquirer—should be the TRA exemption for qualifying standard transactions. As a merchant, you'll generally be closer to your customers and so may be able to judge when a transaction may qualify. Bear in mind, however, that acquirers and issuers can apply TRA only if their total fraud exposure across all of their merchant customers falls below specified fraud rate exemption (FRE) limits.

As part of your SCA exemption strategy, you should carry out fraud screening on transactions before you submit them for authentication and subsequent authorization. During the fraud screening process, you can:

- Request an exemption
- Submit the transaction via EMV® 3DS for potential application of SCA

Your checklist for developing an SCA exemption strategy:

1. **Align with your payment gateway and acquirer to ensure your SCA exemption strategy will be supported.** Remember you need agreement from your acquirer to use the TRA exemption.
2. **If you carry out sophisticated fraud risk screening, work with your acquirer to develop a strategy for applying the acquirer TRA exemption.**
3. **Make sure you understand your acquirer's fraud rate.** Consider changing acquirers if you would benefit from the application of exemptions to higher-value transactions.
4. **Cybersource Decision Manager plus Payer Authentication allows merchants to set up rules around authentication requests.** If a transaction is out of scope or an exemption is available, the solution will pause the authentication call and send the transaction straight to authorization.

   If the issuer declines the exemption request and requires authentication, you must manage this process with your customer; and resubmit successfully authenticated transactions for authorization. By late 2022, this process will be automated in the Cybersource solution to further reduce SCA friction.

Disclaimer: Timelines are subject to change depending on adjustments to Cybersource's release schedule.

Manage SCA declines

Even when a transaction appears to qualify for an exemption from SCA, the merchant may receive an SCA decline from the issuer. This means the issuer has declined to authorize the transaction and requires it to be resubmitted with an authentication request.

There are two main reasons for SCA declines:

1. **The issuer doesn't agree that the transaction is low risk. With greater visibility of transactions across many merchants, the issuer may have more insight than you do into the riskiness of a transaction.**

2. **You requested TRA on a transaction where the value exceeds the issuer's own upper limit. For example: the transaction value is €300 / £265, but the issuer supports TRA on transactions up to €250 / £220 only.**

If you receive an SCA decline, you should submit it with an authentication request within the same payment session and, if authentication is successful, retry for authorization. This process will be automated with Cybersource Decision Manager plus Payer Authentication by late 2022.

You should agree with your payment gateway and acquirer on how best to manage SCA declines and resubmissions.

Disclaimer: Timelines are subject to change depending on adjustments to Cybersource's release schedule.

How the right fraud solutions can help

A sophisticated fraud management solution can help you recognize and flag transactions that are out of scope for SCA, or may qualify for an SCA exemption.

Using a solution like Cybersource Decision Manager—combined with our Payer Authentication solution for EMV® 3DS—to screen transactions before you submit them for authorization, allows you to:

- **Build business rules** to identify transactions that are out of scope for SCA or may qualify for an SCA exemption.
- **Request exemptions** for qualifying transactions:
  - Bypass authentication and move straight to transaction authorization with an exemption request
  - Authentication with an exemption request
- **Use business rules** to request (or bypass) authentication for one leg out (OLO) and other transactions where SCA isn't required by regulation.
- **Handle SCA declines** by retrying with authentication requests. By late 2022, this process will be automated in Cybersource Decision Manager plus Payer Authentication to help deliver an even more seamless customer experience and better protect against potential lost sales.

Disclaimer: Timelines are subject to change depending on adjustments to Cybersource's release schedule.

Get in touch

Our integrated suite of fraud management solutions helps you accept more good orders and give genuine customers a great experience. All while keeping fraud under control, in our PDS2 SCA era.

Would you like to talk through options?
We're here for you.

Find out how we can help by visiting, cybersource.com.

Contact us

> "Cybersource takes a holistic approach to help a merchant solve a challenge or take advantage of an opportunity. We have the breadth of tools and knowledge to help develop a solution to deliver the best results."

Mari-anne Bayliss, Cybersource

Flexible, creative solutions for everyday life

Cybersource helped kick start the eCommerce revolution in 1994 and haven't looked back since. Through global reach, modern capabilities, and commerce insights, we create flexible, creative commerce solutions for everyday life—experiences that delight customers and spur growth globally. All through the ease and simplicity of one digital platform to manage all payment types, fraud strategies, and more. Knowing we are part of Visa and their security-obsessed standards, you can trust that business is well taken care of—wherever it may go.

cybersource
A Visa Solution

cybersource.com

All brand names and logos are the property of their respective owners, are used for identification purposes only, and do not imply product endorsement or affiliation with Visa. DISCLAIMER: Case studies, statistics, research, and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial, or other advice. You should consult with your legal counsel to determine what laws and regulations may apply to your circumstances. The actual costs, savings, and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties, and assumptions that are difficult to predict or quantify. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy, or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental, or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.