Fraud Screening in the Age of Strong Customer Authentication (SCA)

CyberSource®
A Visa Solution

Strong customer authentication (SCA) will be required from September 2019. This paper helps to explain when and how it applies, how liability may work, and why SCA doesn't replace merchants' own fraud screening programs.

While PSD2, the revised Payment Services Directive, came into force in January 2016, with rules being applied from January 2018[1], the regulatory standards take effect from 14 September 2019. Key among them is SCA, a form of multi-factor authentication designed to help prevent fraudulent payment transactions.

Why SCA doesn't replace fraud screening

The introduction of SCA doesn't mean merchants should stop screening for fraud. You should continue screening for fraud to maintain your fraud rates — regardless of whether or not you remain liable for fraud on any given transaction. A merchant's ability to influence the use of transaction risk analysis (TRA) — which allows some transactions to be exempted from SCA — depends on their overall fraud rate staying below specific thresholds. If you raise your acquirer's average fraud rate, you can expect more transactions to be challenged or declined, and you may incur penalties as a result of falling foul of scheme rules.

[1] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/law-details_en

Introduction to SCA

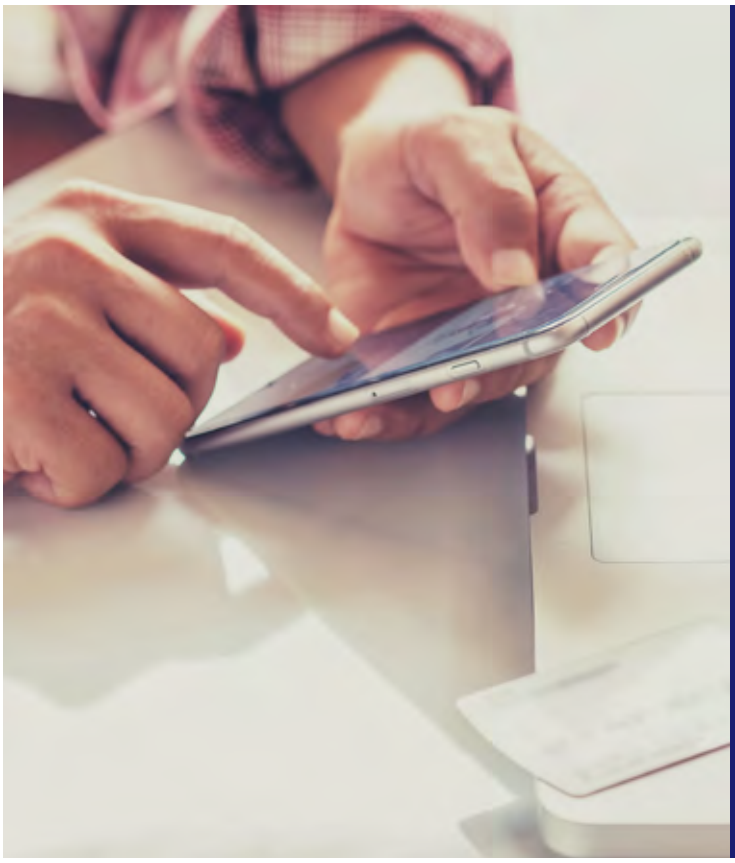
When SCA comes into force, it will be mandatory on electronic payment transactions, except for those deemed out of scope of SCA, or where an allowed exemption is applied to an in-scope transaction.

Out-of-scope transactions

The following transaction types are out of scope for SCA:

- Transactions in the MOTO[2] channel
- Merchant-initiated transactions, such as direct debits
- One-leg-out (OLO) transactions
- Recurring transactions with a consistent amount, once the first transaction has been authenticated

You will need to maintain a good fraud prevention program for them, you should also bear in mind that when fraud becomes harder in one channel, fraudsters may migrate to another: so be on the lookout for increased fraud in the MOTO channel when SCA comes into effect.



What is SCA?

SCA secures an electronic payment transaction by requiring the consumer to present two or more of the following;

Something they know,
eg a one-time password, PIN

Something they have,
eg a token generator,
mobile device, plastic card

Something they are,
eg thumbprint, voice match

[2] See the glossary at the back for more on all of the acronyms in this paper.

SCA exemptions

Sometimes transactions that are in scope for SCA may be exempted from authentication. According to PSD2, only acquirers (PISPs) and issuers (ASPSPs) can exempt transactions from SCA. But merchants can influence an acquirer's decision, as we explain in the next section.

Table 1 shows three key allowed SCA exemptions.[3]

Table 1. Key SCA exemptions

Exemption allowed if	Exemption applied by
Transaction value is less than €30. But the issuer **must** overrule this exemption once a card: • Accumulates five transactions without a challenge for SCA (ie, the sixth transaction must be challenged) or • Reaches a cumulative value of more than €100 without an SCA challenge (a challenge for SCA will reset the card's counter to zero)	Acquirer (PISP) at own decision or on behalf of the merchant or Issuer (ASPSP)
The beneficiary has been whitelisted by the paying customer with their bank.	Issuer (ASPSP)
After carrying out transaction risk analysis (TRA), the acquirer or issuer decides that the transaction doesn't need to be challenged. TRA may be applied to transactions up to €500.	Acquirer (PISP) or Issuer (ASPSP)

What is transaction risk analysis (TRA)?

TRA applies to transactions with a value of up to €500. Acquirers (PISPs) and issuers (ASPSPs) can apply TRA only if their total fraud exposure across all of their customers falls below specified fraud rate exemption (FRE) limits.

	Fraud rate exemption (%)	
Transaction value (euros)	Remote card payments	Credit transfers
250–500	0.01	0.005
100–250	0.06	0.010
0–100	0.13	0.015

TRA is effectively what the majority of 3-D Secure (3DS) providers already do when they use risk-based analysis to decide whether or not to challenge a transaction.

[3] We have not included a complete list of allowed SCA exemptions. For a full list see: Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1523371602118&uri=CELEX:32018R0389

How to influence the application of exemptions

Although PSD2 says that only acquirers (PISPs) and issuers (ASPSPs) can apply SCA exemptions, there are two potential ways to influence your acquirer's actions, and these will also indirectly affect issuer authentication decisions.

1. Agree an exemption strategy with your acquirer

You should agree an exemption strategy with your acquirer so that they honor your choices. Agree what will happen not just when you want an exemption triggered, but also when you prefer *not* to take advantage of an allowed exemption (for example, to benefit from a liability shift).

Bear in mind that if your acquirer agrees to allow you to initiate exemption decisions, you'll probably be liable for those transactions, so you'll want to maintain an effective fraud detection program. It's much the same scenario as authorizing transactions today and forgoing the liability shift of 3DS: good fraud detection is the only way to reduce fraud and liability on these transactions.

2. Take on TRA responsibility

If you have an effective fraud management program, you could discuss with your acquirer the idea of their sub-contracting to you their TRA responsibility for your transactions. If your acquirer allows it (and your acquirer meets the fraud rate exemption criteria for TRA — see below), this may give you greater control over when and when not to apply the TRA exemption on your transactions.

What about the issuer?

Even when your acquirer flags a transaction as exempt, the issuer may override the exemption — if there's a good reason to do so. In practice, they can always override; and they may always run their own TRA process to make that decision. But they're unlikely to routinely step up transactions for SCA without a genuine reason, as customer friction is no more in their interests than it is in yours.

The role of an effective fraud detection program

Although your influence over issuer behavior may be indirect, it's real. It's unlikely that you'll see unexpected issuer challenges as long as you:

- Have an effective fraud detection program, with low reported fraud rates
- Ensure (in collaboration with your acquirer) that exemption flags aren't, as a rule, raised for risky transactions

SCA and fraud liability

PSD2 doesn't have the final say over where fraud liability falls in all potential scenarios. Rather, it's down to agreements among card schemes, acquirers, issuers and merchants to specify liability terms.

We can, however, make some reasonable assumptions about how fraud liability may play out, given the likelihood that acquirers and issuers will use 3DS as their TRA process. Our assumptions outlined below are intended for general information purposes only and do not constitute legal advice or other professional advice or an opinion of any kind.

Out-of-scope transactions

For transactions that are out of scope for SCA, 3DS will remain an avenue for liability shift.

In-scope transactions

Liability will rest with the acquirer, issuer, or even the merchant, depending on the situation. See Table 2.

Table 2. Fraud liability for in-scope transactions

Situation	Who is liable	Explanation
SCA occurs (ie, issuer steps up the transaction)	Issuer	The issuer will be liable as they are responsible for carrying out customer authentication.
Acquirer doesn't raise an exemption flag: • Either overriding merchant exemption request • Or at merchant request • Or at own decision if merchant expresses no preference	Issuer	The issuer will be liable whether they step up the transaction for SCA or exempt it based on TRA, whitelisting, or for any other reason.
Acquirer flags a transaction as exempt	The acquirer will likely pass any liability back to the merchant, unless there is a different agreement in the contract	Depending on scheme rules, the acquirer will go down one of the following routes when submitting to the issuer: • Exempt + authorize[4] • Exempt + authenticate In both instance, if the issuer approves without stepping up the transaction for SCA, the acquirer will be liable.

[4] If the issuer declines, the acquirer will resubmit via the 'exempt+authenticate' route.

Fraud screening to protect your brand

The introduction of PSD2 and SCA doesn't change the need for merchants to protect their brand reputation, and their customers' experience, by maintaining an effective fraud screening program for both in- and out-of-scope transactions.

In a nutshell, if you don't screen for fraud, you could be exposing yourself to fraud. Simply relying on acquirers or issuers to carry out TRA will be no more of a remedy than relying exclusively on 3DS today. The reality is that you are in the best position to implement a strategy relevant to your business, that takes account of the behavior of your customers, to keep fraud rates under control in all of your channels.

In the age of SCA (as with 3DS today), even when you are not liable for fraud, your fraud rate will still count against you with acquirers, issuers, and scheme rules. Issuers and acquirers may be even more ill-disposed towards merchants with rising fraud rates than they are today, because their ability to use TRA as an exemption route at all depends on maintaining overall low fraud rates across all of their customers.

As a result, if you stop screening for fraud you may soon see an increase in challenged or declined transactions. Merchants who take this route shouldn't be surprised if they also lose customers as a result.

Glossary of key terms

ASPSP	account servicing payment service provider (issuer)
FRE	fraud rate exemption
MOTO	mail order / telephone order channel
OLO	one leg-out — transactions are described as OLO when any one of the following applies: • The card is issued outside of the EU • The customer's bank is outside of the EU (for credit transfers) • The merchant isn't domiciled in the EU
PISP	payment initiation service provider (acquirer)
PSD2	revised EU Payment Services Directive, in force since 13 January 2018
SCA	strong customer authentication (multi-factor authentication)
TRA	transaction risk analysis

More information about the PSD2 SCA regulation

All information in this paper relating to the PSD2 SCA regulation is correct as of June 2018. For full details see: Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

Contact us

Email. europe@cybersource.com www.cybersource.co.uk

CyberSource is a global, modular payment management platform built on secure Visa infrastructure with the benefits and insights of a vast $427 billion global processing network. This solution helps businesses operate with agility and reach their digital commerce goals by enhancing customer experience, growing revenues and mitigating risk. For acquirer partners, CyberSource provides a technology platform, payments expertise and support services that help them grow and manage their merchant portfolio to fulfill their brand promise. For more information, please visit www.cybersource.com

CyberSource®
A Visa Solution