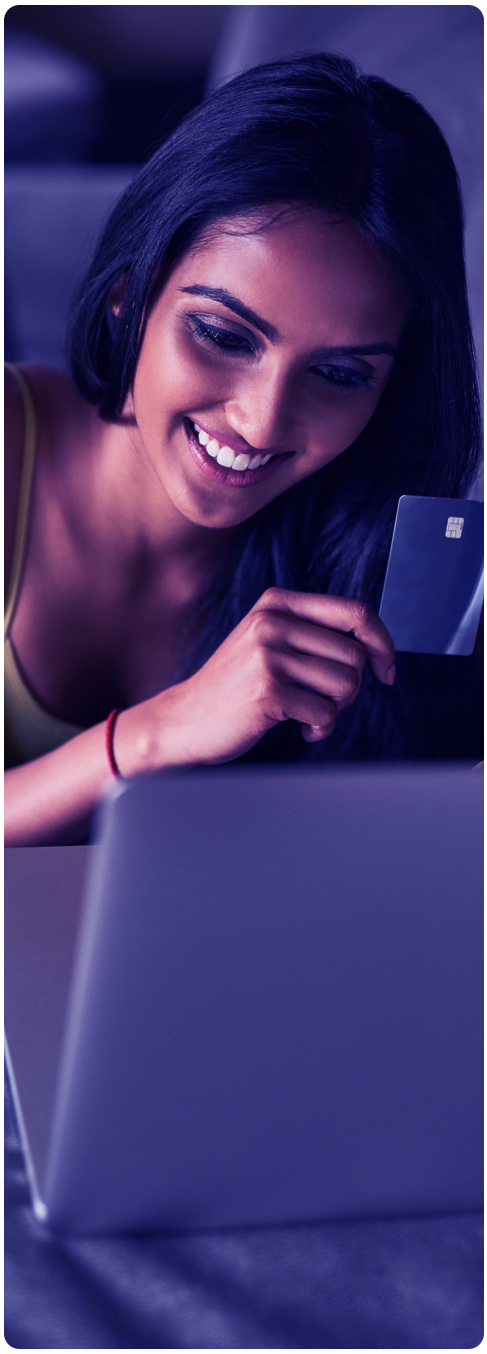


PSD2 and Strong Customer Authentication (SCA)

A Merchant Guide

ACI Worldwide
Real-Time Payments

Executive Summary

With the second Payment Services Directive (PSD2) firmly established in Europe since January 2018, payment markets around the world are readying themselves for the imposition of Regulatory Technical Standards (RTS) for strong customer authentication (SCA). Originally due to come into force on September 14, 2019, the deadline for compliance has now been extended for eCommerce card payments to December 31, 2020.

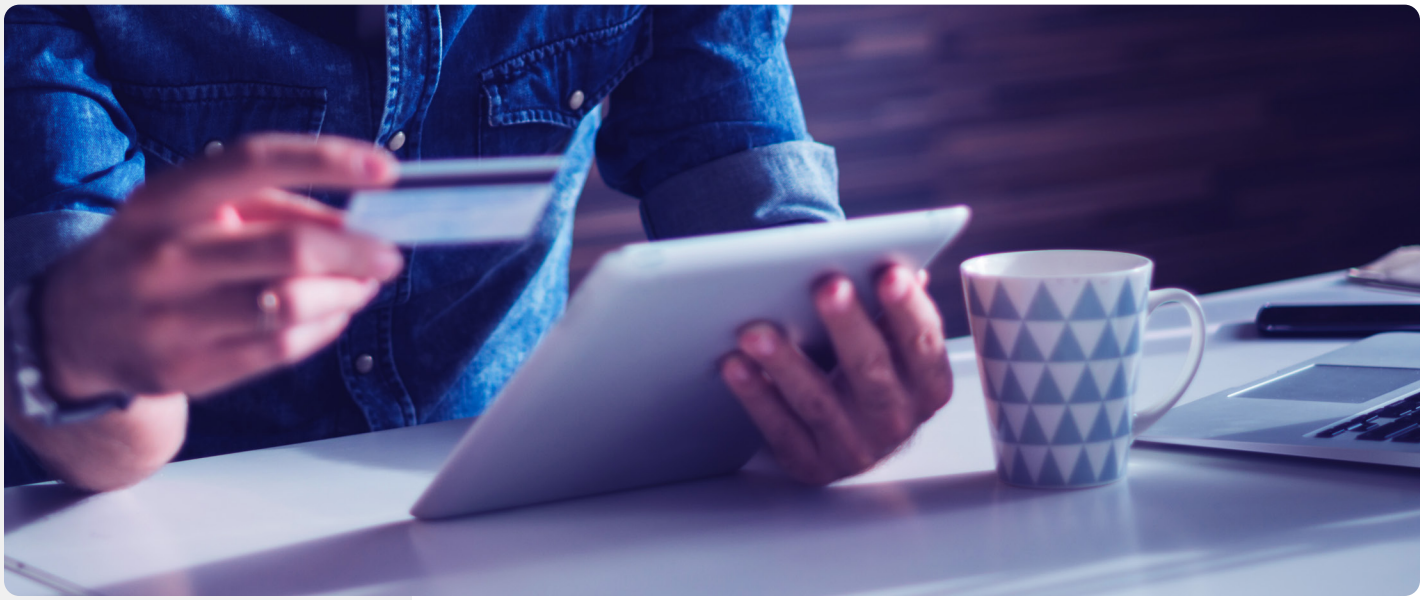
What does this mean for merchants — and what do you need to do to protect your customers, your reputation and your business?

1 Background

PSD2 was established to drive payments innovation and data security by reducing competitive barriers, mandating new security processes and encouraging standardized technology to protect the confidentiality and integrity of payment service users' personalized security credentials.

Although consumers will see tremendous benefit around security and data protection, issuers, acquirers and merchants will face new challenges. One of the requirements within PSD2 is SCA — to ensure that fraud is reduced and merchants and issuers in the European Economic Area (EEA) are validating the consumer for all electronic payments.

The purpose of this paper is to outline the issues and requirements with potential solutions for impacted merchants.



2 What Is SCA?

The security measures outlined in the RTS stem from the key objective of PSD2 to ensure consumer protection. The RTS introduces requirements that issuers and acquirers must observe when they process payments or provide payment-related services.

In general terms, card issuers will be obliged to perform an SCA check for every electronic payments transaction above €30 that does not meet any one of a set of specified exemption criteria. The SCA check requires authentication using two of the following factors:

Something the cardholder knows
— e.g., a password or PIN

Something the cardholder has
— e.g., a token, a mobile phone

Something the cardholder is
— e.g., a fingerprint or voice match

While card issuers can try to reduce the number of cases in which SCA is required, there is no way to prevent it fully. And, importantly, merchants cannot fend off the SCA mechanism for card payments — because their bank no longer has a free choice on whether or not to perform SCA. In cases where the issuer is required to perform SCA, the merchant must also support it, or the issuer has to soft decline the authorization request.

3 When Is an SCA Check Required and What Are the Exemptions?

SCA checks are mandated for every electronic payment over €30 — and for those under €30 where either there have been five previous transactions on the same card without SCA being applied or the card has accumulated transactions totaling more than €100 without an SCA check being applied.

Transactions out of scope for SCA include recurring transactions (after the first transaction has been authenticated), MOTO, one-leg-out transactions (where the card is issued or the merchant is based outside the EEA) and direct debits.

...merchants cannot fend off the SCA mechanism for card payments — because their bank no longer has a free choice on whether or not to perform SCA.

Transactions that are in scope may be rendered exempt from SCA if the cardholder has applied to have the merchant with which they are transacting white-listed with their bank (card issuer), and the bank has agreed. Under PSD2, individual cardholders may ask their issuers to "white-list" merchants they use regularly — but the decision will ultimately be at the bank's discretion — and will depend on the level of fraud exposure the bank has experienced with the chosen merchant.

Issuers and acquirers may also render a transaction that is under €500 exempt if they have demonstrably low levels of fraud. This requires that transaction risk analysis (TRA) is in place and fraud is kept below set exemption threshold values (ETV). These values are:

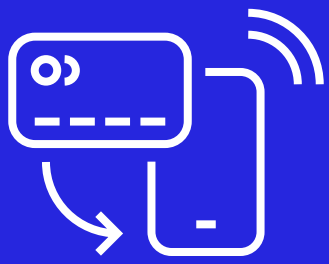
- 0.13% for transactions up to €100
- 0.06% for transactions up to €250
- 0.01% for transactions up to €500

It is expected that issuers will apply the TRA exemption as much as possible to reduce the friction and frequency of SCA that their cardholders will encounter during remote purchases.

In some cases, issuers may request SCA even if the acquirer has implemented an exemption — if they are suspicious about the transaction.

Only issuers and acquirers can exempt a transaction from SCA. There are exemption flags in 3DS for a merchant to request an exemption.

For a full list of exemptions, see the **final report** of the draft RTS.



4 Who Is Liable for Fraud?

For transactions that are subject to SCA, liability rests with the issuer or acquirer. Whoever applies the exemption is then liable for that transaction. In some circumstances, where it applies an exemption, an acquirer will likely pass liability back to the merchant. Merchants therefore need to continue to manage fraud, irrespective of authentication and in case of pushback by the issuer.

5 EMV 3D Secure 2.1/2.2

The advice to merchants from card schemes and most issuers is to implement the latest version of 3D Secure, which is rolling out in 2019 as the primary authentication method used to meet SCA requirements for card payments.

EMVCo (the joint venture overseen by the six major card associations: American Express, Discover, JCB, Mastercard, UnionPay and Visa) first published the specs for EMV 3D Secure 2.0 in 2016. Version 2.1 was designed to improve the shopping experience for customers, including frictionless authentication and shorter transaction times. It uses 10 times more data than 3DS 1.0 and improves the overall user experience. The latest version, 2.2, which is currently in development, includes support for exemptions for additional types of frictionless authentication including acquirer/issuer transactional risk assessment, white- listing, and low-value, one-leg-out and merchant- initiated transactions.

According to projections from the card networks, with EMV 3D Secure Version 2, merchants will be able to achieve the same performance levels as physical store merchants using chip and PIN. But this theory has yet to be put to the test in real-world conditions.

The broader rollout of 3DS adoptions by geographic region is as follows:

- April 2019: Mastercard issuers globally and European Visa issuers can support 3D Secure Version 2 in their production environments.
- August 2019: Visa issuers in North and South America can support 3D Secure Version 2.
- April 2020: Issuers from the rest of the world can support 3D Secure Version 2.
- December 31, 2020: PSD2 SCA goes into effect in European markets.

6 Best Practices for Merchants

As noted above, PSD2 requires that fraud rates are assessed at the payment provider level, not for the individual merchant. For transactions to be exempt from SCA, this means a merchant's fraud rate must remain low enough not to pull the overall fraud rate of the issuer or acquirer over the documented threshold. If the issuer's or acquirer's overall fraud level exceeds that dictated by PSD2, then every eCommerce transaction, regardless of amount and of individual merchant performance, will have SCA applied and exemptions will not be allowed.

So, what does this mean for merchants?

- First, merchants should continue to screen for fraud to de-risk transactions and protect their customer relationships. Merchants understand the business and behaviors of their own customers and hold significant amounts of transactional data which can be used by their fraud prevention partners to profile customers and monitor for fraud. It isn't enough to rely on issuers and acquirers to carry out risk analysis — any more than it is enough to rely on 3D Secure alone. The merchant's ability to control fraud, secure SCA exemptions and deliver a fast, simple payments experience to loyal customers ultimately demands that they keep a firm grasp on fraud rates.

Retaining a strong fraud solution also helps the merchant to avoid penalties incurred for exceeding fraud levels defined in scheme rules.

- Issuers and acquirers will take a keen interest in the level of fraud a merchant experiences, since this directly impacts their own overall fraud levels, and we may see these payment service providers "cherry picking" merchants with a good track record on fraud losses. Where they do not continue to fraud screen — and, so, to provide evidence of low fraud rates — merchants should be prepared for an increase in challenges and declines as payment providers seek to hold down their own fraud levels.

- Retaining a strong fraud solution also helps the merchant to avoid penalties incurred for exceeding fraud levels defined in scheme rules. All merchants will need to be able to perform SCA where issuers request authentication and to prevent fraud on transactions that are out of scope of the regulations.

- Secondly, merchants would be well advised to ensure they are in a position to switch acquirers, route transactions to acquirers with the best fraud levels and negotiate acquiring services. Some merchants may wish to negotiate with acquirers to implement transaction risk analysis exemptions for themselves and, in the future, we could see savvy merchants "cherry picking" the acquirers that offer the best conversion, SCA strategies and commercials.

- Finally, merchants should actively engage with their acquirers to discuss their authentication strategy — and to ensure there is a backup plan or fallback position in the event that authentication fails. PSD2 and SCA have been designed with the expectation that merchants will actively seek exemptions and it is critical that merchants fully understand, and push for, the exemptions that they want and that are available to them. There may be situations in which a merchant does not wish an available exemption to be applied and the exemption strategy should therefore be jointly agreed upon between the merchant and acquirer. It is again important to note that if a merchant applies for an exemption and it is granted by the acquirer, the merchant may become liable for the transaction.

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ATL1346 07-21

ACI Worldwide
Real-Time Payments