PSD2 and Strong Customer Authentication (SCA)

An issuer guide

ACI Worldwide
Real-Time Payments

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). Although the Euro Banking Association has provided an update on SCA timelines for eCommerce card payments—with a new hard deadline for migration completion of December 31, 2020 (original deadline of September 14, 2019), this does not mean that the pressure has been lifted. Issuers should use the new timelines to ensure they have implemented best practice, value-added solutions ahead of the deadline. Following publication of the EBA's Opinion, issuers now have a timeframe in which to implement SCA exemptions in a way that differentiates their business from the competition.

What does this mean for issuers—and what do issuers need to do to better their account holders and grow the 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.

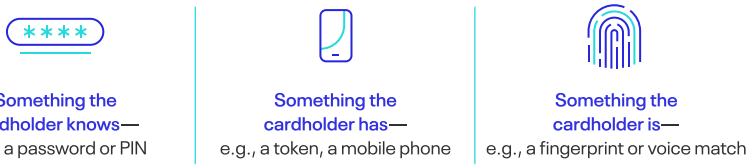
The purpose of this paper is to outline the issues and requirements for issuers—and the consumers they serve.

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 (referred to in the regulations as "payment service providers") must observe when they process payments or provide payment-related services.

SCA differs from current authentication methods which often involve a static password combined with a one-time password (OTP) delivered by SMS. This experience can be a frustrating customer experience if the consumer regularly transacts with a merchant. SCA exemptions can be used to alleviate current payments friction, without increasing risk.

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:



While card issuers can try to reduce the number of cases in which SCA is required, there is no way to prevent it fully. Merchants cannot opt out of or choose to override the SCA mechanism for card payments—because their acquirer 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 may choose to soft decline the authorization request, or defer the liability to the merchant or acquirer.

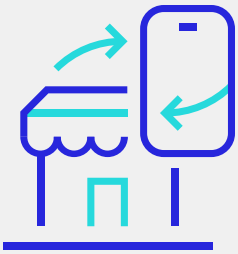
It's crucial for issuers to prioritize the implementation of SCA exemptions in order to meet their customer protection requirements, and uphold their customer experience. Without SCA exemptions, issuers risk additional friction in the payments process, and relegation to back of wallet.

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

SCA exemptions are an important part of the balancing act between protecting transactions and providing a seamless customer experience. For many card issuers, this could be a key customer experience differentiator. For organizations that do not successfully implement SCA exemptions, it could negatively impact their frictionless payment aims and encourage customers to use cards from other providers for online purchases.

SCA aims to standardize practices across the EEA and reduce fraud, especially in the case of online transactions. It requires two independent sources of validation known as two-factor authentication (2FA). This increased security obviously benefits banks and merchants, but if not implemented effectively, risks negatively impacting customer experience, with repercussions including cart abandonment. To mitigate this risk and at the same time improve customer experience, RTS does provide a number of exemptions to SCA, aimed at minimizing friction. Some of these include:

- Low-value payments exemption (below €30)
- Recurring payments exemption, such as subscriptions
- Trusted beneficiaries, including identified trusted merchants Secured corporate payments
- Transactions that real-time transaction risk analysis (TRA) solutions have identified to be low-risk



Low-value payments

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 challenge or the card has accumulated transactions totaling more than €100 without an SCA check being applied.

Recurring payments

Transactions out of scope for SCA include recurring transactions (after the first transaction has been authenticated), MOTO, one-leg-out transactions and direct debits.

Secured corporate payments

Where a corporate card is "lodged" with a contracted third party, for example, the details of corporate cards used for managing employee travel, expenses are often held by the approved travel agent and can be charged with fees after an employee has reserved flights or hotels. This particular exemption is expected to have a relatively narrow scope of applicability for the majority of issuers.

Trusted beneficiaries

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 whitelisted with their bank (card issuer), and the bank has agreed. Under PSD2, individual cardholders may ask their issuers to "whitelist" 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 and individual TRA.

Transaction risk analysis

Issuers and acquirers may also exempt a transaction under €500 if they have demonstrably low levels of fraud. This requires that 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

If an acquirer cannot demonstrate a fraud rate below these thresholds, then all transactions processed on that issuer's cards will be subject to SCA. This would be detrimental to the issuer's market share, as undoubtedly customers would migrate to card issuers that provide a more seamless customer experience. Therefore, a strong SCA strategy is one that encompasses robust TRA and exemptions.

The issuer and acquirer relationship

Issuers and acquirers should seek to apply the TRA exemption to all qualifying transactions to reduce friction and lessen the frequency of SCA that their cardholders will encounter during remote purchases. It's about creating a positive customer experience with their merchant, payments instrument and provider of choice, to remain "front of wallet" and encourage consumer spending.

In some cases, issuers may instigate a soft decline and 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. This means the liability sits with the banks.

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

4 Who Is Liable for Fraud?

Liability for any fraud depends on how the transaction was authenticated.

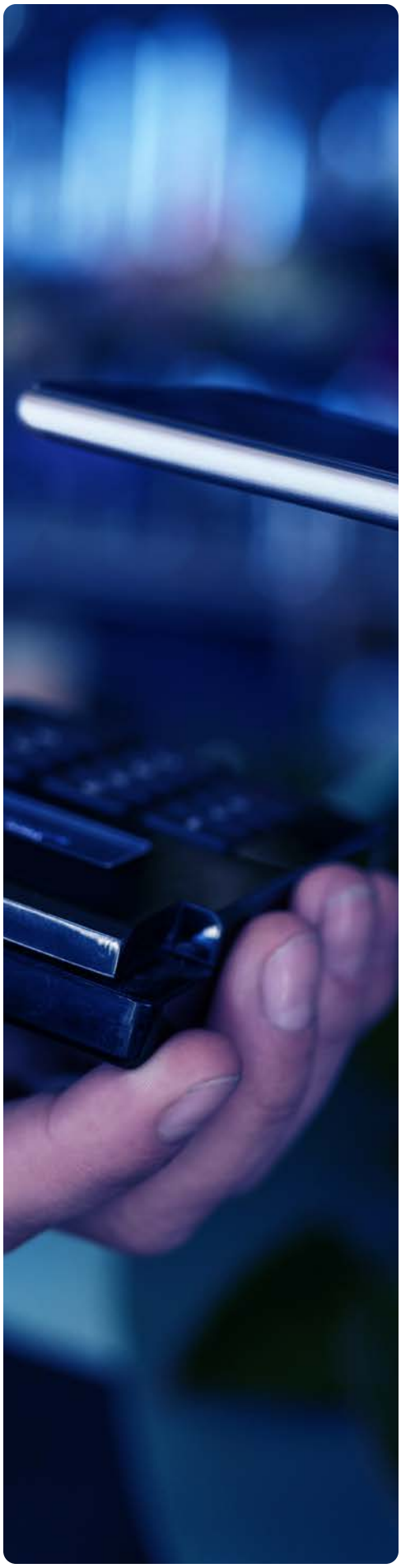
In a standard transaction flow, as today, where the merchant is 3DS-enabled, the issuer retains liability for any fraud. If the merchant is not 3DS-enabled, the acquirer is liable for the fraud but will likely pass this to the merchant, just as many merchant acquiring relationships function currently.

As we move into an SCA exemptions scenario, it becomes more complex. Where the issuer and merchant have "both legs in" the EU and the merchant initiates 3DS, the acquirer may choose to apply an exemption. But if the issuer chooses to overrule the acquirer and conduct SCA, then the issuer assumes liability. However, if the issuer accepts the acquirer's exemption and does not step-up the authentication, then the acquirer is liable for any fraud; it's likely the acquirer would pass that loss on to the merchant as is the current model.

Merchants will need to manage fraud (either directly or through their merchant services partner), irrespective of authentication in order to manage push back by the issuer.

It's critical that acquirers understand the liability implications and conduct robust TRA under Article 18 in order to be confident of their application of SCA exemptions. If an issuer is not compliant by the deadline, the potential consequences include: loss of license, fines or designation as a non-compliant party, and a halt placed on their business. Issuers should use the new deadline extensions as an opportunity to implement SCA exemptions alongside TRA capabilities in order to continue to provide exceptional customer experience once SCA mandates come into effect.

The new "legs in, legs out" scenarios have caused ambiguity in the market. The card schemes are actively looking to clear any confusion and will provide educational materials regarding liability. Once issuers fully understand their roles, they can better guide their customers. There is not a good enough understanding of the impact and benefits of SCA at the merchant and consumer levels. Issuers and acquirers should look to work with the schemes in educating their customers to better mitigate liability.



Use Case	Merchant	Liability
Standard 3DS	Initiates 3DS	Issuer
Merchant not 3DS-enabled	Cannot apply 3DS	Acquirer/Merchant
Merchant/PSP/ acquirer exemption	Initiates 3DS flow with exemption	Issuer if step-up
Merchant/PSP/acquirer SCA	Authenticates consumer with SCA	Issuer if step-up

5 EMV 3D Secure 2.1/2.2

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 issuer/acquirer TRA, whitelisting, low-value, one-leg-out and merchant-initiated transactions.

It is in issuers' best interests to ensure that their access control server (ACS) provider is equipped for the latest version of EMV 3D Secure as the primary authentication method. The richer data and extended fields are necessary to provide SCA exemptions for card payments. In a standard SCA flow, the payments gateway or PSP will look to secure the SCA or exemptions response from the issuer via the directory's integration into its ACS provider.

There is also a benefit to merchant customers leveraging the latest version of EMV 3D Secure, according to projections from the card networks. Merchants will be able to achieve the same performance levels as physical store merchants using Chip and PIN. It will be interesting to see this theory put to the test in real-world conditions.

For online purchases, merchants seem to be favoring EMV 3DS as the "go-to" method of authentication through their PSPs or acquirers (via the payments gateway) to create flexibility in their choice to leverage SCA exemptions where appropriate. This makes real-time decisioning based upon those richer data fields even more crucial for issuers. Competitors will be capitalizing upon this capability for their own exemptions strategy.

There appears to be a grey area regarding merchant mobile apps and a wide variety of customer experiences in this scenario. The typical route of a one-time password does not seem to apply here. We are beginning to see a move towards leveraging inherence in the form of biometrics, alongside digital wallets and PINs in order to combine with SCA. There are some alternative use cases in discussion in the market, although they are yet to be confirmed.

6 Best Practices for Issuers

PSD2 requires that fraud rates are assessed at the issuer or acquirer level, not by the individual merchant. This means that issuers must begin to prepare for SCA ahead of the completion deadline. If issuers do not enable SCA exemptions, they run the risk of impacting the consumer experience and negatively impacting revenue for all parties in the payments value chain. Educating both merchants and consumers on the benefits of SCA is critical to success of the issuer's exemptions strategy.

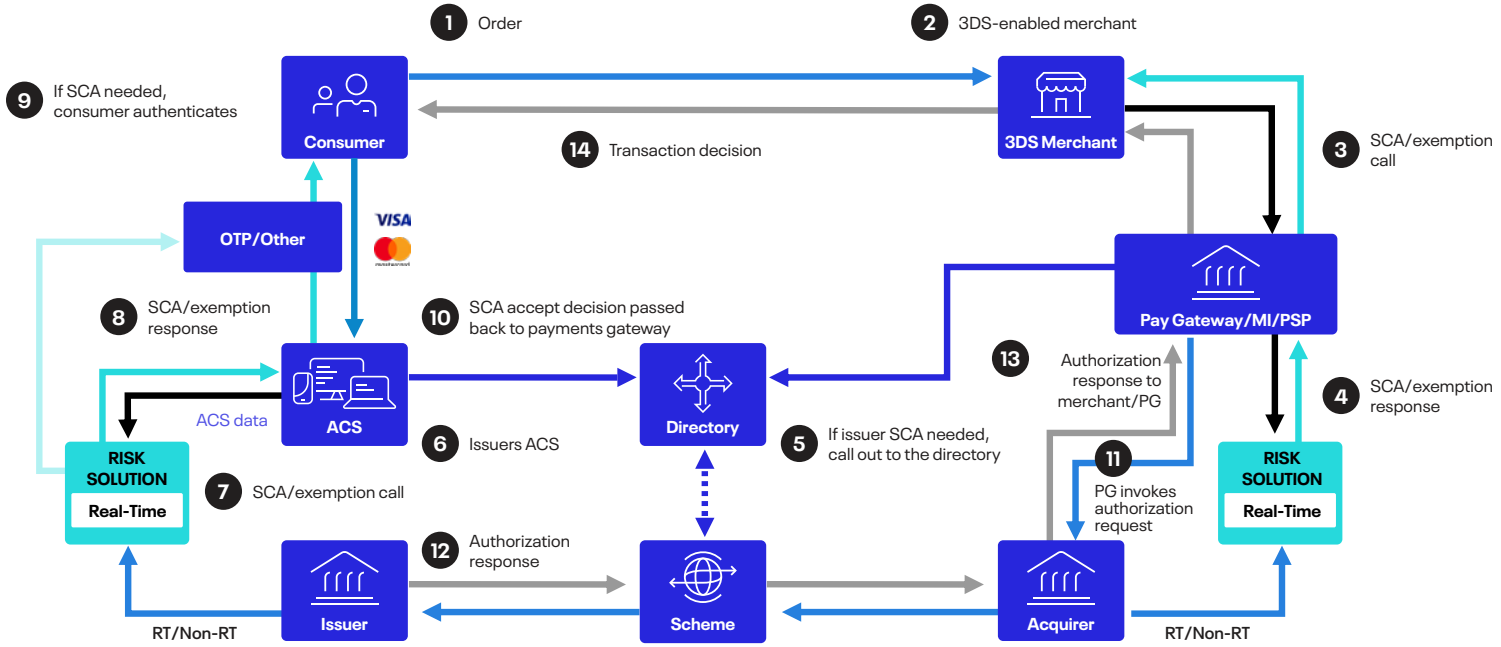
Even if issuers have already begun to implement their SCA strategy, they must re-evaluate it against the new EBA Opinion document. For online purchases, EMV 3DS in combination with a one-time password via SMS or email will no longer be acceptable. This will require some issuers to pivot their SCA strategy. A combination of a PIN/static password with a one-time password—to satisfy the need for both knowledge and possession—may be one of the simplest routes to compliance. It's likely that in the mobile channel, issuers will look to leverage biometrics from the device for a combined possession and inherence approach. Bringing the authentication strategies and authentication messages into a single solution allows for more sophisticated rules, adaptive machine learning models, behavioral biometrics data, better investigation and reduced false positive rates.

The most urgent priority for issuers is to implement solutions that allow them to handle exemptions criteria. ACSs, which manage the EMV 3DS flows, must be integrated with fraud solutions to allow them to ingest authorization messages for TRA and SCA exemptions. Fraud solutions must also operate with real-time capabilities to ensure that customers can transact online instantly. Real-time decisioning on SCA is critical to a successful exemptions strategy; there can be no latency in either an SCA or exemptions application. A single solution should be leveraged with capabilities for SCA exemptions plus other fraud capabilities, as well as payment flows for authorizations, chargebacks, settlement, postings, etc. Solutions must include the ability to simply configure SCA and exemptions codes in order to continually optimize the customer experience.

Issuers should build a strategy and timeline for compliance to adhere to the December 31, 2020 deadline. The extension beyond September 14, 2019 allows issuers to re-evaluate their strategy and ensure they are implementing in a way that will add value to their customers. SCA exemptions should be a part of issuers' launch plans for SCA, not seen as a later phase. Compliance must be balanced with customer experience.

PSD2 RTS-SCA and Exemptions—EMV 3DS Scenario

Both legs in (issuer and merchant both in the EU)



7 How Issuers Can Achieve SCA Success

1. Identify, accept and embrace the need for SCA and an exemptions strategy.
2. Adopt the best approach and strategy on how to engage the right technology partner to assist.
3. Implement before the deadline.

Find out what these changes mean for acquirers.

Download PSD2 and Strong Customer Authentication (SCA)

An acquirer guide

Download Now

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

ATL1137 04-21

Want to know more?

Learn how ACI® Fraud Management™ can help issuers achieve compliance and manage customer experience in parallel to minimize the impact of SCA and capitalize on the opportunity of exemptions.

Read More

ACI Worldwide
Real-Time Payments