



# PSD2 and Strong Customer Authentication (SCA)

An acquirer guide



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 at the time of writing, deadlines are under review and are set to be extended perhaps as far out as September 2021 (as has already happened in the U.K.). This does not mean that the pressure has been lifted. Acquirers should use the new timelines to ensure they have implemented best-practice, value-added solutions to comply ahead of the deadline. Following publication of the [EBA's Opinion](#), acquirers 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 acquirers—and what do acquirers need to do to better serve their merchant base 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 acquirers—and the merchants 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.

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 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 organizations to realize the benefits of SCA by rapidly implementing differentiated services that bring added value to acquirers and merchants.

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

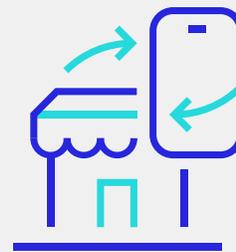
SCA exemptions are an important part of the balancing act between protecting transactions and providing seamless customer experience. For many financial services firms that provide merchant acquiring services, this could be a key differentiator. For organizations that do not successfully implement SCA exemptions, it could negatively impact the business of their merchants and risk market share loss in the process.

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 not if 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 acquirers.

### **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:

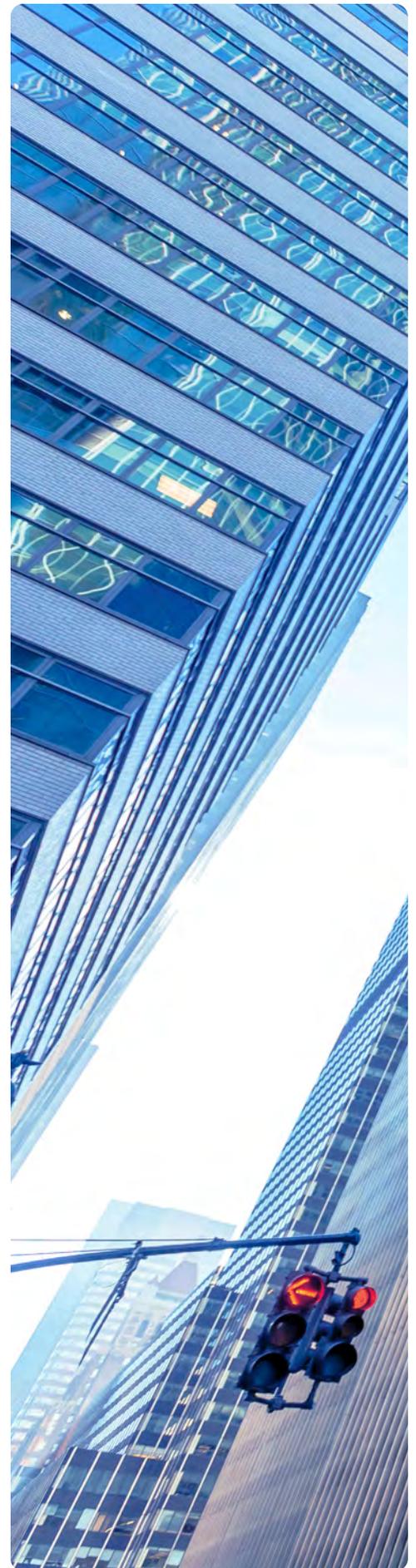
- 0.13% for transactions up to €100
- 0.06% for transactions up to €250
- 0.01% for transactions up to €500

If an acquirer cannot demonstrate a fraud rate below these thresholds, then all transactions processed via that acquirer will be subject to SCA. This would be detrimental to the acquirer’s market share, as undoubtedly merchants would look to acquirers that can provide exemptions for 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 acquirer or PSP is not compliant by the deadline, the potential consequences include: loss of license, fines or designation as a non-compliant party, and a halt is placed on their business. Acquirers should use the new deadline extensions as an opportunity to implement SCA exemptions alongside TRA capabilities in order to continue to differentiate their merchant services once SCA mandates come into effect.

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





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 acquirers fully understand their roles, they can better guide their merchants and PSPs/payment gateway providers. There is not a good enough understanding of the impact and benefits of SCA at the merchant and consumer levels. Acquirers and issuers should look to work with the schemes in educating their customers to better mitigate liability.

## 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, includes support for exemptions for additional types of frictionless authentication, including acquirer/issuer TRA, whitelisting, low-value, one-leg-out and merchant-initiated transactions.

It is in acquirers’ best interests to ensure that the latest version of 3D Secure is available for their merchants as the primary authentication method, whether directly or via PSPs. The richer data and extended fields are necessary to provide SCA exemptions for card payments.

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.

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 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 Acquirers

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

Providing value-added merchant services to manage exemptions is critical as a competitive differentiator and can be rapidly and easily adopted at the acquirer level with the right technologies and partners. Acquirers must also be cognizant of rising merchant fraud and consider this in their exemptions strategy. Acquirers should actively engage with their PSPs and merchants to discuss their authentication strategies. 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 between the merchant and acquirer.

Even if acquirers have already begun to implement their SCA strategy, they must re-evaluate it against the EBA's June 2019 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 acquirers 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, acquirers 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. Integration with access control server (ACS) solutions and payment gateways for real-time decisioning on SCA is critical to a successful exemptions strategy.

Deadline extensions are not an excuse for acquirers to put their feet up—this time should be treated as an opportunity to accelerate their readiness. The extension allows acquirers to re-evaluate their strategy and ensure they are implementing in a way that will add value to their business. SCA exemptions should be a part of acquirers' launch plans for SCA, not seen as a later phase. Compliance must be balanced with customer experience.





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](http://www.aciworldwide.com)

@ACI\_Worldwide

[contact@aciworldwide.com](mailto:contact@aciworldwide.com)

Americas +1 402 390 7600

Asia Pacific +65 6334 4843

Europe, Middle East, Africa +44 (0) 1923 816393

© Copyright ACI Worldwide, Inc. 2021

ACI, ACI Worldwide, ACI Payments, Inc., ACI Pay, Speedpay and all ACI product/solution names are trademarks or registered trademarks of ACI Worldwide, Inc., or one of its subsidiaries, in the United States, other countries or both. Other parties' trademarks referenced are the property of their respective owners.

ATL1139 04-21

#### Want to know more?

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

[Read More](#)