LTO GLOBAL PROCESSING

STRONG CUSTOMER AUTHENTICATION AND 3-D SECURE

FREQUENTLY ASKED QUESTIONS

24 NOVEMBER 2020

Table of Contents

1. Overview

1.1 What is PSD2?

The second European Payment Services Directive (PSD2) is a European directive which came into force across the European Economic Area (EEA) on January 13, 2018. 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.

PSD2 requires banks to support Open APIs to enable consumers to make payments directly from their bank accounts via newly-regulated third-party payment service providers. However, the primary focus of this document is the introduction of the Regulatory Technical Standards (RTS) around strong customer authentication (SCA). These standards came into effect on September 14, 2019.

1.2 What is Secure Customer Authentication (SCA)?

The security measures defined around SCA introduce 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 specified exemption criteria. The SCA check requires authentication using two of the following three 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

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

1.2.1 Is there any flexibility on the September 14, 2019 deadline?

In response to industry uncertainty and unreadiness for the September 14, 2019 secure customer authentication (SCA) deadline, the European Banking Authority (EBA) have issued two opinion papers on secure customer authentication:

- *Dated June 21, 2019: Elements of strong cutomer authentication under PSD2*
- *Dated October 16, 2019: Deadline for migration to SCA for eCommerce payment transactions*

The first opinion paper concludes that the *national competent authority (NCA) of each European country* may work with merchants and payment service providers (PSPs) to "provide limited additional time" for issuers, acquirers and merchants to migrate to SCA-compliant solutions. This flexibility is contingent on PSPs having a migration plan agreed with their NCA, and on the quick

execution of that plan. This initial proposal led to concerns of a divergent European regulatory environment posing challenges to organizations operating internationally.

The second opinion paper recommended that migrations to SCA-compliant solutions, including merchant testing and implementation, should be completed by December 31, 2020. This opinion also strongly encouraged a consistent approach towards the SCA migration period across European NCAs.

While we expect the majority of NCAs to ultimately follow the EBA guidance, they are recommendations rather than firm requirements. The latest position from NCAs are available below for reference.

- **Austria:** *The Financial Market Authority (FMA)* has confirmed that Austria will align with the 15-month transition period proposed by the EBA opinion.
- **Belgium:** *The National Bank of Belgium* confirmed before the EBA opinion that they would "work in close cooperation with the industry stakeholders" on a migration plan and a timetable.
- **Bulgaria:** *The Bulgarian National Bank* confirmed directly to financial institutions that they will align with the 15-month transition period proposed by the EBA opinion.
- **Croatia:** *Hrvatska Narodna Banka* has confirmed that Croatia will align with the 15-month transition period proposed by the EBA opinion.
- **Cyprus:** *The Central Bank of Cyprus* has confirmed that Cyprus will align with the EBA transition period. This transition period is no longer limited to entities supporting non-reusable and non-replicable elements such as one-time passwords, superseding their previous position.
- **Czech Republic:** *The Czech National Bank* has confirmed that the Czech Republic will align with the 15-month transition period proposed by the EBA opinion.
- **Denmark:** *Finanstilsynet* has confirmed (albeit not in writing) that Denmark will align with the EBA timeline, rather than their previously-communicated 18-month transition period. They have also stepped back from their initial limitation to solutions using OTP via SMS and card details. They will however allow flexibility until January 11, 2021 to avoid holiday-season disruptions.
- **Estonia:** *Finantsinspektsioon* have acknowledged the EBA's new date, after stating prior to the EBA opinion that they would align with the transition period duration proposed by the EBA.
- **Finland:** *The Financial Supervisory Authority* has confirmed that Finland will align with the 15-month transition period proposed by the EBA opinion.
- **France:** *Banque de France* initially confirmed that the EBA deadline was in line with their own timelines. However, a gradual ramp-up of soft declines until June 2021 is now expected.
- **Germany:** *BaFin* has confirmed that Germany will formally maintain the EBA's December 31, 2020 deadline, although there will be a ramp-up period of soft declines until March 15, 2021.
- **Greece:** *The Bank of Greece* stated prior to the EBA opinion that they would align with the transition period duration proposed by the EBA.
- **Hungary:** *Magyar Nemzeti Bank* have aligned with the EBA deadline, which replaces their previous 12-month transition. However, PSPs are expected to adhere to the timelines of any migration plans they have already submitted.
- **Ireland:** *The Central Bank of Ireland (CBI)* will provide a progressive ramp-up of soft declines until April 1, 2021.
- **Italy:** *Banca d'Italia* will implement a ramp-up soft decline plan, with SCA to be enforced for all transactiosn from April 1, 2021.
- **Latvia:** *The Financial and Capital Market Commission* has confirmed that Latvia will align with the 15-month transition period proposed by the EBA opinion.

- **Lithuania:** *The Bank of Lithuania* stated prior to the EBA opinion that they would align with the transition period duration proposed by the EBA.
- **Luxembourg:** *The Commission de Surveillance du Secteur Financier (CSSF)* has confirmed that Luxembourg will align with the 15-month transition period proposed by the EBA opinion.
- **Malta:** *The Central Bank of Malta* has confirmed that Malta will align with the 15-month transition period proposed by the EBA opinion.
- **The Netherlands:** *De Nederlandsche Bank (DNB)* has confirmed that the Netherlands will align with the 15-month transition period proposed by the EBA opinion.
- **Norway:** *Finanstilsynet* has confirmed that Norway will align with the 15-month transition period proposed by the EBA opinion.
- **Poland:** *The Polish Financial Supervision Authority* has confirmed a transition period, and has stated that the maximum duration would be provided following the EBA opinion.
- **Portugal:** *Banco de Portugal* has confirmed that Portugal will align with the 15-month transition period proposed by the EBA opinion.
- **Romania:** *Banca Națională a României* has confirmed that Romania will align with the 15-month transition period proposed by the EBA opinion.
- **Slovakia:** *Slovak National Bank* stated prior to the EBA opinion that they would align with the transition period duration proposed by the EBA.
- **Slovenia:** *Banca Slovenije* has confirmed that Slovenia will align with the 15-month transition period proposed by the EBA opinion.
- **Spain:** *Banco de España* has confirmed that Spain will align with the 15-month transition period proposed by the EBA opinion.
- **Sweden:** *Finansinspektionen* has confirmed that Sweden will align with the EBA's 15-month transition, superseding their original position that there would be no transition period. PSPs who have already submitted migration plans should submit amended plans in light of the EBA opinion.
- **United Kingdom:** *The Financial Conduct Authority* has announced that they will provide until September 14, 2021 for SCA implementation, as a result of the impact of the COVID-19 crisis.

In recent correspondence with industry leaders, **the European Commission indicated that the December 31, 2020 deadline for secure customer authentication (SCA) remains in place, with no provisions made for an extension.** While the European Commission acknowledged the challenges of COVID-19 for merchants, they highlighted the significant increase in online payments as "[calling] more than ever before for robust and innovative strong authentication methods."As such, merchants and PSPs operating in these markets are recommended to continue to work to the December 31, 2020 deadline.

1.2.2 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 transactions (Mail/Telephone order)
- One-leg-out transactions (where the card is issued or the merchant is based outside the EEA)
- Direct debits

Note that for recurring (or other merchant-initiated) transactions, customers will need to ensure that they are submitting these transactions with the appropriate credential-on-file indicator. These transactions may otherwise be soft-declined, causing the transaction to fail as the shopper is not present to authenticate.

While card issuers can try to reduce the number of cases in which SCA is required, there is no way to prevent it fully. In cases where SCA is required but does not take place, the issuer has to soft decline the authorization request.

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.

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.

1.2.2.1 Is fraud screening still required?

Merchants are encouraged to continue screening their transactions in order to keep their fraud rate low. This means that the acquirer, who is responsible for fraud scoring across the breadth of their merchant base, can grant TRA exemptions to merchants who are effectively managing their fraud levels.

1.2.2.2 What happens with fraud liability in the case of exemptions?

The liability for transactions will sit with the issuer when a transaction has been authenticated using SCA. The liability remains with the issuer if the issuer applies a TRA exemption to SCA. When an exemption to SCA is applied by the acquirer using a TRA exemption, the liability will be transferred to the acquirer, unless the issuer challenges the transaction.

1.2.2.3 Should SCA be applied for one-leg out or recurring transactions?

One-leg-out transactions are those where either the issuer or the acquirer are located outside the European Economic Area (EEA). While these transactions are out of scope for SCA, it is expected that SCA should be applied on a 'best effort' basis.

As for recurring transactions, any transactions/installments after the initial authorization are flagged as merchant-initated transactions (MIT). MIT is out of scope for SCA, and as such it does not need to be applied. This applies even if the initial authorization did not go through SCA.

1.2.3 Is there any effect to card-present (CP) transactions?

While the majority of requirements around SCA relate to card-not-present (CNP) transactions, SCA will also be required for some card-present (CP) contactless payments based on value and velocity. Contactless transactions are exempt from SCA if they meet the following conditions:

- Payments over €50 in Europe, or £50 in the United Kingdom; and
- Five consecutive payments without consumer authentication; or
- Cumulative payments to the value of €150 without consumer authentication

A majority of cards currently in circulation were not implemented with these velocity limits, which is expected to be rectified in the device implementation.

1.3 What is 3-D Secure?

3-D Secure is a customer authentication protocol introduced by EMVCo and leading card schemes, designed to reduce fraud rates and provide security to merchants and shoppers for card-not-present transactions. 3-D Secure V1 is already widely in use today, but does not enforce modern secure authentication methods and frequently relies on archaic authentication methods such as static passwords.

1.3.1 What is 3-D Secure V2?

3-D Secure V2 is the latest version of the 3-D Secure protocol. 3-D Secure V2 includes several key changes to the handling of card-not-present payments. Critically, these changes ensure the protocol is fully in line with the PSD2 regulatory technical standards around SCA, which come into effect on September 14, 2019. Furthermore, the updated protocol is designed to help streamline the customer journey by reducing or removing points of friction, ultimately improving checkout conversion rates as well as reducing fraud.

1.3.2 What are the benefits of 3-D Secure V2 compared to previous versions?

There are several benefits to merchants, issuers and shoppers as a result of 3-D Secure V2. Broadly, the changes ensure a streamlined customer journey with fewer friction points to reduce the high rate of shopping cart abandonment from 3-D Secure V2. These enhancements include:

- **Risk-based authentication.** 3-D Secure V2 will support the transmission of additional rich data during transactions, making authentication assessments and decisions more accurate. The issuer will be able to evaluate the fraud risk and bypass full authentication if the risk is low enough, resulting in a smoother customer journey for low-risk shoppers. This risk-based approach to authentication is entirely aligned with PSD2 guidance on SCA.

- **Biometric or two-factor authentication.** If the issuer (after performing an initial assessment) determines that authentication is required, either biometric or two-factor authentication will be performed to validate the shopper. The biometric authentication methods available will depend on what is supported.

- **Eliminates initial enrollment.** The removal of this one-time step in the 3-D Secure flow eliminates a major point of friction in the customer journey upon first-time use.

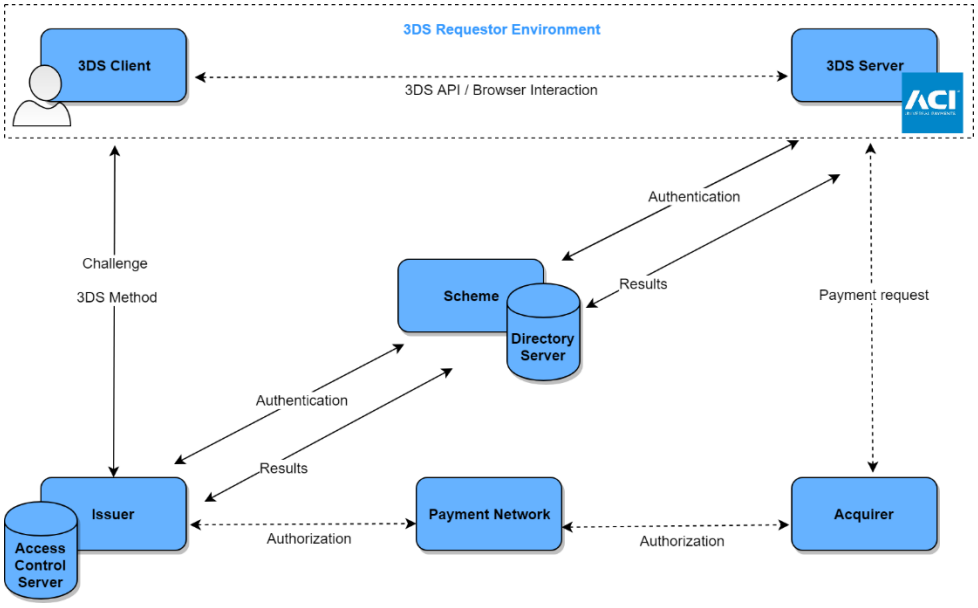
- **Support for in-app purchases.** Unlike 3DS V1, which required a browser call-out to complete authentication, 3DS V2 can handle in-app purchases natively. This avoids compatibility issues experienced within some apps for browser authentication callouts.

- **Allows for bespoke checkout integration.** Should they wish, merchants can now integrate the 3-D Secure authentication process into their own checkout process, resulting in a much smoother experience for shoppers.

- **Support for non-payment authentications.** The latest 3-D Secure version offers support for no-value authorizations, such as tokens for card-on file. Note that it is mandatory to perform an SCA check such as 3-D Secure to add a new card as a card-on-file. Subsequent transactions do not have to go through 3-D Secure, but need to reference the original transaction and the amount cannot differ by more than 15%.

1.3.3 What are "frictionless flow" and "challenge flow"?

As mentioned previously, risk-based authentication based on rich data is a key feature of 3-D Secure V2. If the issuer determines the transaction is low-risk, they can bypass full authentication altogether – this is referred to as "frictionless flow". If the issuer decides to go ahead with full authentication, this triggers what is known as the "challenge flow", which more closely mirrors the 3-D Secure V1 workflow.



In the authentication phase, the 3DS server sends information about the cardholder to the directory server. It is then forwarded on to the correct access control server, which performs a risk check to determine next steps.

If risk is determined to be low, the payment continues with no further interaction between the issuer and cardholder. This is **frictionless flow.**

If the issuer decides the shopper needs additional authentication, the cardholder interacts with the issuer to authenticate themselves biometrically or using two-factor authentication. This is the **challenge flow.**

1.3.4 Will 3-D Secure V1 remain available?

ACI will continue to support 3-D Secure V1 alongside V2, until further notice from card schemes on timings for deprecation of the older version.

1.3.5 What are "the differences between 3-D Secure 2.0, 2.1 and 2.2?

The specs for EMV 3-D Secure 2.0 were first published by EMVCo in 2016, with subsequent versions adding additional functionality. Version 2.1 introduced frictionless authentication, shorter transaction times, and uses 10 times more data than version 1.0.

The payments ecosystem is currently adapting to the latest version (2.2), which includes support for exemptions for additional types of frictionless authentication. This includes acquirer-side transactional risk assessment, whitelisting of merchants, transaction retries after 'soft deny' responses, and support for decoupled and requestor-initiated authentication. Current plans for future versions include further enhancements to transaction risk assessment and support for devices other than web browsers and mobile devices.

1.3.6 Will merchants require new merchant IDs (MIDs)?

It is important to differentiate between two types of merchant IDs:

- The first type of merchant ID is assigned by the acquirer, and will not change as a result of implementing 3-D Secure V2.

- The second type of merchant ID is assigned by the schemes, and is also frequently referred to as a 'Requestor ID'. If the merchant is already enrolled for 3-D Secure V1, the same merchant ID can be retained for 3-D Secure V2. However, the Requestor ID will not be automatically enrolled for 3-D Secure V2. As such, the merchant or their PSP will need to ensure that their Requestor ID is enrolled with the scheme, or a new merchant ID will need to be requested.

1.3.7 Is an upgrade to 3-D Secure V2 required, and if so when by?

1.3.7.1 Europe

Customers in Europe are strongly recommended to migrate to 3-D Secure V2 by December 31, 2020, the enforcement deadline for PSD2 regulatory technical standards across Europe. This is because 3-D Secure V2 offers support for exemptions and enforcing of secure authentication methods. Mastercard reporting on UK Finance's interpretation of the EU-wide regulatory technical standards describes this as offering merchants "operational readiness".

Transactions in the EEA that do not meet SCA requirements (those that do not pass through 3-D Secure or equivalent authentication) are liable to be declined by the issuer after this date.

1.3.7.2 Rest of world

Visa and Mastercard have mandates in place that encourage the adoption of 3-D Secure V2 for issuers. Mastercard have mandated this for issuers globally from April 1, 2019, whereas Visa have confirmed the following schedule:

- April 12, 2019: Europe
- August 15, 2019: North America and Latin America
- April 18, 2020: Rest of World