
STORM-7 CONSULTING
PSD2
REGULATION AND INNOVATION
CUSTOMER AUTHENTICATION

Storm-7 Consulting
Rodrigo Zepeda
CEO, Storm-7 Consulting

PSD2 Transaction Thresholds for Strong Customer Authentication

There are two main drivers underlying the revised Payment Services Directive (**PSD2**), enhanced consumer protection and the need to encourage competition among financial providers. Under the PSD2 there is an increased focus on Strong Customer Authentication (**SCA**). Whilst the PSD2 took effect from 13th January 2018, there has been a transitionary period in place as the rules regarding the use of SCA will only apply from 13th September 2019. From this date all remote electronic payments made within the European Economic Area (**EEA**) where the cardholder's bank and the business's payment provider are both situated within the EEA will require SCA, which is essentially Two-Factor Authentication (**2FA**). This will differ from the present situation whereby SCA is only required on an exception basis, where the risk of the transaction is regarding as 'high' then additional authentication may be triggered, referred to as 'step-up'. The SCA rules are contained within the Final Report Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2) which were published on 23rd February 2017 (**Draft RTS**).

SCA and 2FA

2FA is an additional security layer that helps to address the vulnerabilities of a standard password-only approach. For example, withdrawing money from an Automated Teller Machine (**ATM**) requires 2FA as it requires a physical bank card (i.e. something the individual possesses) and the use of the correct Personal Identification Number (**PIN**) (i.e. something the individual knows). Exceptions to this SCA requirement include cash payments and payments made using a physical card at a Point of Sale (**POS**) terminal. The SCA procedure requires satisfaction of at least two factors from two distinct categories, namely:

(1) knowledge (i.e. something an individual personally knows such as a passcode, alphanumeric code, password);

(2) possession (i.e. something an individual personally possesses such as a smartphone, tablet, smartwatch, hardware token);

(3) inherence (i.e. something personal to an individual such as a fingerprint, facial recognition, voice characteristics, retina scan, detection of unique behavioural patterns such as keystroke analysis).

The 2FA process results in the generation of an authentication code that can be accepted only once by the Payment Service Provider (**PSP**) when the Payer:

(1) uses the authentication code to access its payment account online;

(2) initiates a payment transaction;

(3) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

In the case of remote electronic payment transactions (**EPTs**) SCA must include elements which 'dynamically link' the transaction to a specific amount and a specific payee.

3D Secure 2

'3D Secure 2' (**3DS2**) which is the new version of 3D Secure will be the primary authentication method used to meet SCA requirements for card payments. Currently the most common way of authenticating a card payment relies on '3D Secure 1' (**3DS1**), which is an authentication standard supported by most major card networks (examples include 'Verified by Visa' and 'Mastercard SecureCode'). SDS1 is set to be decommissioned in 2020.

Visa and Mastercard have stipulated that the new 3DS2 should be in place for issuers and merchants by April 2019, and the 3DS2 specifications have been released by EMVCo. One of the major changes

that 3DS2 brings is that it offers the ability to authenticate transactions using biometric methods. The use of biometric methods will potentially reduce the amount of fraud in payment transactions whilst at the same time potentially offering consumers a more convenient payment experience.

3DS2 will also not feature the additional payment windows offered through 3DS1 which often led to more friction for paying customers. Under 3DS1 only cards could be used for payment by consumers whereas under 3DS2 consumers can now also use mobile payments and digital wallet payment methods which will significantly increase convenience for consumers whilst at the same time increasing security of payments.

Exemptions to SCA

Transactions that are initiated by the customer are within the scope of the SCA rules, as well as to electronic payments initiated by the payer through the payee (e.g. credit transfers, including e-money transfers or card payments). However there are a number of exceptions that apply to PSPs (but they cannot be applied at merchant level):

(1) recurring direct debits unless these are set up electronically (as these are considered to be merchant-initiated);

(2) one-leg transactions;

(3) contactless payments at POS;

(4) transport and parking fines;

(5) trusted beneficiaries and recurring transactions;

(6) payments to self;

(7) low-value transactions;

(8) secure corporate payment processes and protocols;

(9) Transaction Risk Analysis (**TRA**).

Contactless Payments at POS

PSPs are exempted from the application of SCA where the payer initiates a contactless electronic payment transaction (**CEPT**) if two conditions are met:

(1) the individual amount of the CEPT does not exceed EUR 50; and

(2) the cumulative amount, or the number, of previous CEPTs initiated via the payment instrument offering a contactless functionality since the last application of SCA does not, exceed EUR 150, or 5 consecutive individual payment transactions.

Transport and Parking Fines

Where the payer initiates an EPT at an unattended payment terminal for the purpose of paying a transport or parking fine then this will be exempt from the SCA requirements.

Trusted Beneficiaries and Recurring Transactions

PSPs are exempt from the SCA requirements where:

(1) the payer initiates a payment transaction where the payee is included in a list of trusted beneficiaries previously created or confirmed by the payer through its account servicing PSP; OR

(2) the payer initiates a series of payment transactions with the same amount level and the same payee.

Payments to Self

PSPs are exempt from the SCA requirements where the payer initiates a credit transfer where the payer and the payee are the same natural or legal person and both payment accounts are held by the same account servicing payment service provider.

Low-value Transaction

PSPs are exempt from the SCA requirements where the payer initiates a Remote EPT (**REPT**) provided that two conditions are met:

(1) the amount of the REPT does not exceed EUR 30; AND

(2) the cumulative amount, or the number, of previous REPTs initiated by the payer since the last application of SCA does not exceed EUR 100, or 5 consecutive individual REPTs.

Secure Corporate Payment Processes and Protocols

PSPs are exempt from the SCA requirements in respect of legal persons initiating EPTs through the use of dedicated payment processes or protocols that are only made available to payers who are not consumers, where the competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those provided for by Directive (EU) 2015/2366.

TRA

PSPs are exempted from the SCA requirements where the payer initiates a REPT identified by the PSP as posing a low level of risk to the transaction monitoring mechanisms referred to in Article 2(1) of the Draft RTS.

Table 1: TRA Conditions

<table>
<tr><th>No</th><th>Area</th><th>Description</th></tr>
<tr><td>1</td><td>EPT Amount</td><td>The amount of the EPT does not exceed the Exemption Threshold Value (ETV) for Remote Card-Based Payments (RCBPs) and Credit Transfers (CTs), corresponding to the PSP's fraud rate for such payment services calculated in accordance with No 4 and up to a maximum value of EUR 500.
<table>
<tr><td></td><td colspan="2">Reference Fraud Rate (%) for:</td></tr>
<tr><td>ETV</td><td>RCBPs</td><td>CTs</td></tr>
<tr><td>EUR 500</td><td>0.01</td><td>0.005</td></tr>
<tr><td>EUR 250</td><td>0.06</td><td>0.01</td></tr>
<tr><td>EUR 100</td><td>0.13</td><td>0.015</td></tr>
</table></td></tr>
<tr><td>2</td><td>EPT Real-time Risk Analysis</td><td>The transaction monitoring mechanisms enable the PSP to perform a real-time risk analysis of the EPT which takes into account, at a minimum, the risk factors set out in Article 2, Paragraphs 3 and 4 of the Draft RTS, and combine them in a detailed risk score enabling the PSP to assess the level of risk of the payment transaction.</td></tr>
<tr><td>3</td><td>EPT Low Level of Risk</td><td>An EPT is identified as posing a low level of risk only where the following conditions (in combination with the risk analysis set out in No 2) are met:</td></tr>
</table>

No	Area	Description
		(a) no abnormal spending or behavioural pattern of the payer has been identified; (b) no unusual information about the payer's device/software access has been identified; (c) no malware infection in any session of the authentication procedure has been identified; (d) no known fraud scenario in the provision of payment services has been identified; (e) the location of the payer is not abnormal; (f) the location of the payee is not identified as high risk.
4	PSP's Overall Fraud Rate	For each type of transaction relating to RCBPs or CTs, the PSP's overall fraud rate covering both payment transactions authenticated through strong customer application or executed under any relevant exemption (under Articles 13 to 16) shall be equivalent or lower than the reference fraud rate for the same type of payment transaction in line with the table in No 1. The overall fraud rate for each type of payment instrument should be calculated as the total value of unauthorised or fraudulent remote transactions, whether the funds have been recovered or not, divided by the total value of all remote transactions for the same type of payment instrument, whether authenticated with the application of SCA or executed under any relevant exemption (under Articles 13 to 16) on a rolling quarterly basis (90 days).
5	Audit Review Assessment	The calculation of the fraud rate and resulting figures shall be assessed by the audit review ensuring that they are complete and accurate.
6	Documentation of Methodology and Model	The methodology and model, if any, used by the PSP to calculate the fraud rates, as well as the fraud rates themselves shall be adequately documented and made fully available to competent authorities upon their request.
7	Competent Authority Notification	The PSP has notified the competent authorities of its intention to make use of the TRA exemption.

PSD2 and Merchant Payments

Historically, merchants were able to decide if they required to authenticate their customers via 2FA for a remote payment transaction. However, under the SCA rules it is the issuers that are responsible for customer authentication. This is an important difference in practice because 2FA adds friction to the customer's checkout experience (i.e. slows the customer's checkout experience down) and may potentially negatively impact conversion rates (e.g. customers may abort a transaction because they may not remember their password).

Historically merchants have placed increased focus on streamlining the purchase and payment process in order to establish a frictionless customer payment experience. There was previously a balance to be made between ensuring a frictionless checkout experience by, for example, not using 2FA, and increased fraud rates. In practice merchants therefore developed transacting scoring capabilities in order to be able to effectively assess the risk associated with each payment transaction. However, it should be noted that applying a method of 2FA such as 3D Secure 1 significantly reduces the likelihood

of fraud, and also shifts the liability for a dispute due from the business to the cardholder's bank. Therefore, merchants have the discretion to route transactions through 3DS enabling them to shift liability in the event of loss.

If a payer's PSP does not require SCA the payer will only be liable for a disputed transaction where it is committing fraud. Also, if either a payer or a payee does not accept SCA, then it will be liable to refund the financial damage caused to the payer's PSP. Depending of the design of the payment experience and operating model, SCA may have different implications to a merchant's business. For remote transactions all transactions under EUR 30 will be excluded from the SCA requirements which reflect the low probability of fraud inherent in such transactions. For remote transactions above EUR 30 the procedure that is to be used will reflect the reference fraud rates of the acquiring bank and the issuer, not the merchant.

For RCBPs then if the Reference Fraud Rate is below 13 basis points there is no requirement for a challenge for transactions of up to EUR 100. If the Reference Fraud Rate is below 6 basis points there is no requirement for a challenge for transactions of up to EUR 250. If the Reference Fraud Rate is below 1 basis point, there is no requirement for a challenge for transactions of up to EUR 500.

In practice merchants will need to develop strategies that optimise for exemptions. These strategies will vary depending on a number of different factors ranging from types of products or services provided, to types of sales channel used, target customer base, and authentication procedures used. The new SCA framework will likely also see changes in the charging structures for merchants by banks.

Level 24/25, The Shard, 32 London Bridge Street, London SE1 9SG