Deloitte.

Is 3D Secure 2 solution for card-not-present transactions compliant with PSD2/RTS?

What is 3DS 2.0

3D Secure 2.0 ("3DS2") is the online authentication solution introduced by EMVCo, which is overseen by the six major card schemes (American Express, Discover, JCB, Mastercard, UnionPay and VISA). It brings a new approach to authentication through risk-based authentication, possibility of biometric authentication solutions and an improved online user experience while addressing many of 3DS 1.0's issues.

The main reason for the change in the current payment process and the process of authentication/authorization of payments results from regulatory requirements laid down by the Regulatory Technical Standards on strong customer authentication and secure communication ("RTS")[1] which enters into force on 14 September 2019. RTS specify selected obligations resulting from PSDS in context of strong customer authentication ("SCA").

In this connection, card schemes recommend and also mandate use of 3DS2, which should represent a regulatory compliant solution for SCA. To be compliant with RTS, impacted subjects have to ensure that every card-not-present ("CNP") transaction undergoes SCA. In this context, 3DS2 represents the industry standard authentication protocol compliant with RTS.

There are exclusions from SCA based on the type of transaction. Out of scope of SCA are merchant initiated ("MIT") transactions, mail order/telephone order ("MO/TO") transactions, and business-to-business transactions on direct channels or transactions where the issuer or acquirer is outside of the European Economic Area.

In addition, RTS contain the possibility not to conduct SCA where exemptions from SCA can be applied. Regarding the e-commerce CNP transactions, there are five types of applicable exemptions – merchant whitelisting, recurring transactions (transaction with the same payee and same amount, not to be confused with *merchant-initiated transactions)*, low value transactions, secure corporate protocols and Transaction Risk Analysis ("TRA") exemption for low risk transactions. However, the payee can never decide whether or not to use an exemption – this decision is up to the payer's payment services provider (issuer) or payee's payment services provider (acquirer). In this connection, it is necessary to say that the payer's payment services provider always makes the ultimate decision whether or not to accept or apply exemption – the payer's payment services provider may revert the application of SCA or to decline the initiation of the respective transaction. The use of exemptions, where applicable is not mandatory; however, it positively affects the customer experience.

[1] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

Exemption provided by different payment processors

In the table below, you can see list of possible exemptions from SCA, their description, and information regarding whether major acquirers / payment processors allow for these exemptions.

Exemption	**Description**	**Adyen**	**Worldpay**	**PayPal**	**Global Payments Europe**
		Supported Y / N / ISSUER			
Low value transactions	Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction provided that the following conditions are met: • the amount of the remote electronic payment transaction does not exceed EUR 30; and • the cumulative amount of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed EUR 100 with no time limit; or • the number of previous remote electronic payment transactions initiated by the payer since the last application of strong customer authentication does not exceed five consecutive individual remote electronic payment transactions.	YES	YES	YES	YES
TRA (Low risk)	To qualify as low risk for the purposes of the TRA exemption, a payment transaction must meet several (cumulative) conditions: • The overall fraud rate for that type of transaction, calculated at the PSP level on a rolling quarterly basis, must not exceed the reference fraud rates for the same type of payment transactions as defined in the RTS on SCA • The amount of the relevant payment transaction is equal to or less than the	YES	YES	YES	YES

	relevant exemption threshold specified in the RTS on SCA, up to €500 - After taking into account specific risk criteria, the transaction does not present characteristics that indicate a higher risk of fraud (such as abnormal behaviour of the payer, abnormal location of the payer, etc.).				
Recurring transactions	Payment service providers shall apply strong customer authentication when a payer creates, amends, or initiates for the first time, a series of recurring transactions with the same amount and with the same payee. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, for the initiation of all subsequent payment transactions included in the series of payment transactions made pursuant to the conditions mentioned above.	NO	NO	YES	YES
Whitelisting	Payment service providers shall apply strong customer authentication where a payer creates or amends a list of trusted beneficiaries through the payer's account servicing payment service provider. Payment service providers shall be allowed not to apply strong customer authentication, subject to compliance with the general authentication requirements, where the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.	ISSUER	ISSUER	ISSUER	ISSUER
Corporate protocols	Payment service providers shall be allowed not to apply SCA, in respect of legal persons initiating electronic payment transactions through the use of dedicated payment processes or protocols that are only made available to payers who are not consumers, where the	ISSUER	ISSUER	ISSUER	ISSUER

	competent authorities are satisfied that those processes or protocols guarantee at least equivalent levels of security to those provided for by PSD2. This exemption may be applied to electronic payment transactions initiated using a card payment, provided that the card payment is “only available to payers who are not consumers” and the competent authority (e.g. FCA) is satisfied that the security levels of the dedicated payment processes and protocols used are “at least equivalent” to those provided for by PSD2 before the PSP uses the exemption.				

What does this mean for merchants

Merchants have to ensure that transactions undergo SCA when applicable. For usage of SCA exemption, the merchant has to send additional data that will help the issuer or the acquirer to determine low risk for the target transaction. The merchant should also provide non-SCA payment flow for transactions out of scope of PSD2/RTS to avoid additional drop in transaction success rates. When transaction undergoes SCA or the issuing bank applies exemption from SCA, the issuing bank is liable for loss (chargeback) in case of fraudulent transaction.

Liability shift

The table below describes in which cases liability shift occurs for specific scenarios.

Situation	**Activity**	**Liability shift**	**Final liability**
SCA required	Issuing bank conducts SCA (or 3DS), or even fails to do 3DS	Yes	Issuer
Acquirer exemption	Issuing bank approves exemption	No	Merchant
	Issuing bank declines exemption	Yes	Issuer
Issuer exemption	X	Yes	Issuer
Out-of-scope (e.g. MIT)	X	No	Merchant

Grace period

Although the date when RTS becomes effective remains 14 September 2019, national competent authorities in some countries (UK, Ireland, Germany, Italy, Netherlands, Austria, Belgium, Malta, Poland, Norway, and we are expecting more to come, including France and Spain) decided to provide for a grace period and gave issuers, acquirers, and merchants more time to adapt to new rules. This also gives time for EMVCo to introduce new authentication methods based on behavioural biometrics that would be considered SCA compliant (so called Risk Based Authentication, which is a part of EMVCo’s 3DS2 standard, was not recognized as inherence factor by EBA, and this left the market with the only possible solution to meet RTS expectation for SCA, i.e. out-of-band challenge flow).

Radek Musílek
Senior Managing Associate
Ambruz & Dark Deloitte Legal s.r.o., advokátní kancelář
rmusilek@deloittece.com

Tomáš Huml
Senior Manager | FSI Technology
Deloitte Advisory s.r.o.
thuml@deloittece.com

Jan Ševčík
Senior Consultant | FSI Technology
Deloitte Advisory s.r.o.
jsevcik@deloittece.com