Dive deep into PSD2

with lawyers

On October 2, we participated in a workshop providing a detailed analysis of the requirements of the so called RTS SCA, specifying the particular details of the PSD2 regulation (Dive deep into PSD2). The workshop was organized by CREOBIS and the professional work of the workshop was directed by Bird&Bird Chief Payment Lawyers Scott McInnes and Adrián Calvo. In the present document we summarize the most important findings of the workshop.

Online BUSINESS TECHNOLOGIES

DIGITIE

Introduction

On October 2, we participated in a workshop providing a detailed analysis of the requirements of the so called RTS SCA, specifying the particular details of the PSD2 regulation (Dive deep into PSD2). PSD2 (Payment Services Directive Revised) is the Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market. RTS SCA is the Commission Delegated Regulation (EU) 2018/389, which sets out the detailed provisions of the PSD2 Directive for strong customer authentication and common and secure open standards of communication (hereinafter referred to as "RTS" for simplicity).

The workshop was organized by CREOBIS and the professional work of the workshop was directed by Bird & Bird Chief Payment Lawyers Scott McInnes and Adrián Calvo. During the workshop, we have used for analysing the requirements: the RTS SCA, the Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC published on 13 June 2018, as well as the consultation document published by the British Financial Conduct Authority (FCA) in September 2018 (Approach to final Regulatory Technical Standards and EBA guidelines under the revised Payment Services Directive PSD2).

In the present document we summarize the most important findings of the workshop.

Strong customer authentication – SCA

First, we are dealing with SCA, that is the strong customer authentication described by the RTS. As a basis for the discussion, we have come back to Article 97 of the PSD2 directive, which specifies the cases in which SCA should be applied. Under this Article, SCA shall be applied where the payer:

- accesses its payment account online;
- initiates an electronic payment transaction;
- performs operations through a remote channel, which can give an opportunity for payment fraud and other abuses.

From the foregoing it is important to point out that SCA should only be used in cases where the payer initiates the operation, including cases when the operation is directed to activities that can generally lead to fraudulent or misleading actions, such as in cases related to a direct debit authorization initiated through a Payment Service Provider (PSP), or the acceptance of a payment request. SCA shall also be applied if a card payment is initiated by the payer via the payee. However, there is no need to apply SCA if a card-based payment is actually initiated by the beneficiary, for example in the case of a monthly card charge of a Netflix subscription of € 9.99. There is another exception, the so called MO/TO (Mail Order/Telephone Order) operations under the paragraph 95 of the PSD2 Preamble, that SCA is not required for paper-based payment transactions, or postal and telephone orders.

According to the 30th definition of Article 4 of the PSD2 Directive, "strong customer authentication" means authentication using at least two elements that can be classified as knowledge (information only known to the user of the given service), possession (something only the user possesses) and inherence (a feature of the user). The EBA stated in its opinion (paragraph 33) that the part of the definition of the SCA defined in the RTS saying that the two factors should belong to one of the above three categories, means that the two factors must belong to two distinct categories. At the workshop we have concluded that this interpretation does not follow the RTS's wording and since the EBA's opinion has no legal effect, therefore, an SCA may be legitimate based on two items of the same category if the authentication meets all other conditions of RTS. However, this type of authentication combination should be utilized cautiously because, for example, the FCA shares the opinion of the EBA, so the use of such authentication procedures may be challenged by a local authority during an audit!

Multiple forums have already raised the issue whether the dynamic password sent in an SMS will be adequate, concerning the requirements of strong customer authentication. In this respect, both the EBA (http://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039) and the FCA have clearly stated: as described in point 20.19, a device can be used as the authentication factor for the category of ownership if it is used to generate a token or to receive a one-time password. The dynamic password received in an SMS is to be considered such a receipt of a one-time password.

Exemptions to the use of SCA

It is an important part of both the RTS and the Directive (Article 98) that SCA is not mandatory in certain cases. The application of the exemption is always determined by the service provider who is authorized to perform or omit the SCA in the given process, which may be different for card or TPP payments. When applying the exemption, full responsibility lies with the provider deciding on the application of the exemption, i.e. as the "weakest link" bears the responsibility for the possible reimbursement obligation.

Article 10 - Payment account information

Concerning this exemption, we have determined that the definition of a payment account is not uniform for all countries, so there may be countries where a savings account is considered to be a payment account. This was confirmed by the 4 October decision of the Court of Justice of the European Union, which stipulates that a payment account is an account that can be directly used to initiate or receive a payment to/from a third party.

According to Paragraph 2 of Article 10 of the RTS, payment service providers can not be exempted from the application of strong customer authentication if more than 90 days have elapsed since the payment service user has last accessed online information about his account. According to the EBA's opinion, the 90-day counter of the exemption should be managed

separately for each provider, that is, all account information service providers (AISPs) and the bank's online channels should have a separate counter. An SCA implemented for other reason (such as a payment initiation) cannot restart the account information counter.

At the workshop we have stated that when a customer accesses his account for the first time through a TPP, then the customer gives his access consent to the TPP and not to the bank. In this case, the bank is not allowed to override the consent (e.g., unilaterally disallow access), the bank must request confirmation – in the form of a strong customer authentication - from the customer, who will either confirm or reject this final confirmation. Based on the interpretation of the regulation, it can be stated that a strong customer authentication at the account servicing bank, is to be considered an explicit consent of the customer. It can also be stated that if the customer has more than one account with the bank and the customer did not specify - when authorizing the TPP's access – the exact account which the authorization refers to, then it is not to be considered anobstacle under the RTS (RTS 32 (3) obstacle) if the bank asks for a clarification concerning the account to which the customer's authorization refers. This same principle can be followed exactly in the case of transfers when selecting the source account. (see FCA 7.136).

The regulation stipulates that in the case of payment accounts, the PSD2 API should provide customers with the same data frame that the customer reaches through the electronic channels provided by the account servicing bank, but this range of data can vary widely from one bank to another. If a bank decides to create APIs conforming the minimum requirements of PSD2, it exposes itself to the risk that TPPs wishing to access a broader data stream will be accessing those by the currently used screen scraping or reverse engineering methods, since in case of data sets beyond the PSD2 regulations, it is not mandatory to conform to the RTS requirements!

In relation to the account information service, the application of SCA can only be waived (Article 10 of the RTS) if the client wishes to check his account balance or history of transactions not older than 90 days, or both. For all queries for more information, SCA should be used. Thus, for example, in case of an internet bank access, it is only possible to waive the SCA if the customer will be allowed to access more data than the data described above only after an SCA has been applied.

Article 13 - Trusted beneficiaries

Pursuant to Article 13 (2) of the RTS, payment service providers shall be allowed not to apply strong customer authentication if the payer initiates a payment transaction and the payee is included in a list of trusted beneficiaries previously created by the payer.

At the workshop it was established that a trusted beneficiary can only be provided through the account servicing bank, but in the case of a trusted beneficiary, SCA will not only be left out for online payments but also if the beneficiary pays personally. So, for example, if someone has

Tesco as a trusted beneficiary, he/she may even pay for any further shop purchases without an SCA. Tesco on the other hand, may also require additional conditions for the omission of the SCA. If for example Tesco decides about the exemption of SCA as a card acceptor, it may require as a precondition for the omission of the SCA the joint presentation of the bank card and the regular customer card. The bank may only provide such additional terms if the fulfilment of these additional terms is equally required for all payment channels.

On the workshop the question of clearly defining the trusted beneficiary was raised. So, sticking to the above example, is it sufficient to provide „Tesco" by name, or only the provision of the name and account number, or other identification stipulated by law (i.e. secondary identification) can be considered a clear definition? During the workshop, we could not reach an agreement on this issue, but the most likely solution is that the scope of the data to be recorded for the trusted beneficiary is to be determined by the account-keeping bank.

Article 17 - Secure Corporate Payment Processes and Protocols

According to Article 17 of the RTS, payment service providers shall be allowed not to apply strong customer authentication to 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 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.

Most Member States have not yet determined whether the application of this exemption is linked to the local authority's authorization or not, and if it is so, then what are the requirements for obtaining such an authorization. The FCA's view is that an FCA authorization is not required to apply the exemption, but if a service provider applies this exemption, it must report it to the FCA. According to the FCA's interpretation, the exemption can only be applied when the corporate system communicates directly with the banking system and cannot be used as an exemption for corporate online banking solutions and physical cards issued to corporate employees. (FCA 20.55-60)

Article 18 - Transaction Risk Analysis

With the entry into force of the PSD2, the concept of fraud has changed, and the definition of cheating in the future will also include unauthorized operations and fraudulent operations concluded by the deception of the consumer. Due to the change, it is advisable to review the monitoring reports on fraud.

If a bank decides to apply the exemption, it is worth monitoring the so-called ePrivacy regulations still under discussion (EUR-Lex - 52017PC0010), which concerns the respect for privacy and the protection of personal data in electronic communications. This legislation can have a serious impact on what data can be collected and used for risk analysis.

Account access without the presence of the customer

Article 36 (5) of the RTS SCA provides that account information service providers must provide – even without the active request of the customer - access four times in every 24 hours to those accounts for which account information providers have valid customer consent. From this access frequency, you can go upwards with an individual agreement. As this requirement does not limit the scope of data to be accessed, it should be made possible to access all data that the client can receive directly from the bank. If an AISP initiates access to the account more than four times within a 24 hour period, without further agreement, than it violates the RTS regulations, as the AISP is responsible for compliance with the number of daily accesses granted based on the text of the RTS.

Conclusion

The workshop clearly pointed out that although the final text of the PSD2 Directive had been published in 2015 and the official final text of the RTS is already known since 13 March 2018, still several practical issues arise on a close-to-daily basis, questions that require serious legal analysis and interpretation.

For our company, professional events such as the Workshop of 2 October 2018 are important because, as a banking system developer, we are expected to transform the requirements of PSD2 and the RTS into software functions, requiring a clear definition and interpretation.

The knowledge gathered on the workshop will be used to develop our DigiTie PSD2 software (see https://www.online.hu/solutions/digitie/digitie-psd2), which will help our banking partners to comply with the PSD2 IT requirements. We hope this study will also help our Readers.

If you have any further questions about the issues of the present study or our DigiTie PSD2 solution, please contact us!

About Online Business Technologies

We are an innovative IT development company specialized in banking technology since 1989.

We provide a wide spectrum of highly flexible solutions necessary for banks to go digital, including modules to join FinTech ecosystems (e.g. PSD2, open APIs, instant payments), e-channel solutions, and state-of-the-art core banking modules to support front- and back-office operations (including account management, credits, deposit, GL etc.)

Our modules can be combined freely, we are able to deliver a standalone solution for a specific task (e.g. PSD2), or a series of modules covering the complete value chain (e.g. credit processes).

Our operations in numbers:

- Nearly 2500 years of banking, financial software development experience
- Our solutions are used by more than 8000 users
- Our solutions are used in more than 1000 branches by our customers
- Our partners serve more than 3 million customers with our solutions

OUR VALUES

UNIQUE COMPETENCE Our experience and professional knowledge in the field of credit institutions and finance is unique among IT providers.

CUSTOMIZED SYSTEMS With the help of our unique development and version management technology, our modules can be customized and implemented rapidly. We also have extensive experience in realizing unique functionality.

HIGH QUALITY Owing to the quality control system covering all of our activities and to the controlled development processes, our systems are of high quality and reliability.

QUICK RETURN Fast launching of developments that save customer resources, increased efficiency in management, flexible response to market trends – these all result in our customers gaining advantage in the rapidly changing financial market.

For more information check out our website: www.online.hu and contact us!

Online Business Technologies

H-1032 Budapest, Vályog street 3. | +36-1-437-0700 | https://www.online.hu/contact