COELHO RIBEIRO E ASSOCIADOS
SOCIEDADE CIVIL DE ADVOGADOS

EBA publishes Draft Regulatory Technical Standards on Strong Customer Authentication under Article 98 of PSD2 Directive

CRA – Coelho Ribeiro e Associados, SCARL

Jaime Medeiros

Portugal

March 2017

EBA has published the Final Report and the Draft Regulatory Technical Standards (RTS) on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)[1]. The draft is now with the EU Commission for adoption and it is expected that RTS will be applicable by Member States 18 months after its entry into force as referred in article 115.4 of PSD2.

The PSD2 Directive established that a payment service provider (PSP) should apply strong customer authentication where the payer:

(i) accesses its payment account online;

(ii) initiates an electronic payment transaction; or

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

Now, the Draft RTS, adopting a technology and business-model neutrality, requires that *where payment service providers apply strong customer authentication in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication based on two or more elements categorized as knowledge, possession and inherence shall result in the generation of an authentication code.* The authentication code shall be accepted only once by the PSP when the payer uses the authentication code.

[1] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

The PSD2 Directive also establishes that, in case of the initiation of electronic payment transactions, PSP should include in the strong customer authentication elements which dynamically link the transaction to a specific amount and a specific payee.

The Draft RTS refers that such dynamic linking shall include security measures that meet each of the following requirements:

(a) the payer is made aware of the amount of the payment transaction and of the payee,

(b) the authentication code generated shall be specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction, and

(c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer.

Any change to the amount or the payee shall result in the invalidation of the authentication code generated.

The Draft RTS also establishes exemptions from strong costumer authentication in case:

1. the payment service is only to access the accounts balance or the last 90 days payment transactions;
2. of contactless electronic payment transactions not exceeding € 50 with a cumulative threshold of € 150,00 or five consecutive transactions;
3. of transport and parking fares;
4. of trusted beneficiaries and recurring transactions, provided some conditions are met, and
5. low-value transactions, not exceeding € 50,00, provided that the cumulative amount, or the number of transactions does not, respectively, exceed € 100 or 5 consecutive transactions.

However, PSP that make use of the exemptions is subject to strict fraud monitoring obligations and shall cease to be exempted from the application of strong customer authentication for a given payment instrument where their monitored fraud rate exceeds some ratios defined in the Drat RTS.

The Draft RTS also addresses matters related to confidentiality and integrity of credentials, and requirements for common and secured standards of communication.