Chapter 1

Strong Customer Authentication and Common and Secure Methods of Communication

Article 18 Transaction risk analysis

(1) Payment service providers shall be allowed not to apply strong customer authentication where the payer initiates a remote electronic payment transaction identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2 and in paragraph 2(c) of this Article.

(2) An electronic payment transaction referred to in paragraph 1 shall be considered as posing a low level of risk where all the following conditions are met:

(a) the fraud rate for that type of transaction, reported by the payment service provider and calculated in accordance with Article 19, is equivalent to or below the reference fraud rates specified in the table set out in the Appendix for ‘remote electronic card-based payments’ and ‘remote electronic credit transfers’ respectively;

(b) the amount of the transaction does not exceed the relevant Exemption Threshold Value (‘ETV’) specified in the table set out in the Appendix;

(c) payment service providers as a result of performing a real-time risk analysis have not identified any of the following:

(i) abnormal spending or behavioural pattern of the payer;

(ii) unusual information about the payer's device/software access;

(iii) malware infection in any session of the authentication procedure;

(iv) known fraud scenario in the provision of payment services;

(v) abnormal location of the payer;

(vi) high-risk location of the payee.

(3) Payment service providers that intend to exempt electronic remote payment transactions from strong customer authentication on the ground that they pose a low risk shall take into account at a minimum, the following risk-based factors:

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.

(a) the previous spending patterns of the individual payment service user;

(b) the payment transaction history of each of the payment service provider's payment service users;

(c) the location of the payer and of the payee at the time of the payment transaction in cases where the access device or the software is provided by the payment service provider;

(d) the identification of abnormal payment patterns of the payment service user in relation to the user’s payment transaction history.

The assessment made by a payment service provider shall combine all those risk-based factors into a risk scoring for each individual transaction to determine whether a specific payment should be allowed without strong customer authentication.