Chapter 1

Strong Customer Authentication and Common and Secure Methods of Communication

[redacted]

Article 4 Authentication code

(1) Where payment service providers apply strong customer authentication in accordance with Regulation 100 of the Payment Services Regulation 2017 (SI 2017/752), the authentication shall be based on two or more elements which are categorised as knowledge, possession and inherence and shall result in the generation of an authentication code.
The authentication code shall be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

The authentication code shall be only accepted once by the payment service provider when the payer uses the authentication code to access its payment account online, to initiate an electronic payment transaction or to carry out any action through a remote channel which may imply a risk of payment fraud or other abuses.

(2) For the purpose of paragraph 1, payment service providers shall adopt security measures ensuring that each of the following requirements is met:

(a) no information on any of the elements referred to in paragraph 1 can be derived from the disclosure of the authentication code;

(b) it is not possible to generate a new authentication code based on the knowledge of any other authentication code previously generated;

(c) the authentication code cannot be forged.

(3) Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures:

(a) where the authentication for remote access, remote electronic payments and any other actions through a remote channel which may imply a risk of payment fraud or other abuses has failed to generate an authentication code for the purposes of paragraph 1, it shall not be possible to identify which of the elements referred to in that paragraph was incorrect;

(b) the number of failed authentication attempts that can take place consecutively, after which the actions referred to in Regulation 100(1) of the Payment Services Regulations

2017 (SI 2017/752) shall be temporarily or permanently blocked, shall not exceed five within a given period of time;

(c) the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter 5.

(d) the maximum time without activity by the payer after being authenticated for accessing its payment account online shall not exceed five minutes.

(4) Where the block referred to in paragraph 3(b) is temporary, the duration of that block and the number of retries shall be established based on the characteristics of the service provided to the payer and all the relevant risks involved, taking into account, at a minimum, the factors referred to in Article 2(2).
The payer shall be alerted before the block is made permanent.
Where the block has been made permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments.

The payer shall be alerted before the block is made permanent.
Where the block has been made permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments.

Where the block has been made permanent, a secure procedure shall be established allowing the payer to regain use of the blocked electronic payment instruments.