Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)

TITLE IV

RIGHTS AND OBLIGATIONS IN RELATION TO THE PROVISION AND USE OF PAYMENT SERVICES

CHAPTER 5

Operational and security risks and authentication

Article 95

Management of operational and security risks

1 Member States shall ensure that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. As part of that framework, payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

2 Member States shall ensure that payment service providers provide to the competent authority on an annual basis, or at shorter intervals as determined by the competent authority, an updated and comprehensive assessment of the operational and security risks relating to the payment services they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

3 By 13 July 2017, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, issue guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 with regard to the establishment, implementation and monitoring of the security measures, including certification processes where relevant.

EBA shall, in close cooperation with the ECB, review the guidelines referred to in the first subparagraph on a regular basis and in any event at least every 2 years.

4 Taking into account experience acquired in the application of the guidelines referred to in paragraph 3, EBA shall, where requested to do so by the Commission as appropriate, develop draft regulatory technical standards on the criteria and on the conditions for establishment, and monitoring, of security measures.

Power is delegated to the Commission to adopt the regulatory technical standards referred to in the first subparagraph in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

5 EBA shall promote cooperation, including the sharing of information, in the area of operational and security risks associated with payment services among the competent

authorities, and between the competent authorities and the ECB and, where relevant, the European Union Agency for Network and Information Security.

Article 96

Incident reporting

1 In the case of a major operational or security incident, payment service providers shall, without undue delay, notify the competent authority in the home Member State of the payment service provider.

Where the incident has or may have an impact on the financial interests of its payment service users, the payment service provider shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident.

2 Upon receipt of the notification referred to in paragraph 1, the competent authority of the home Member State shall, without undue delay, provide the relevant details of the incident to EBA and to the ECB. That competent authority shall, after assessing the relevance of the incident to relevant authorities of that Member State, notify them accordingly.

EBA and the ECB shall, in cooperation with the competent authority of the home Member State, assess the relevance of the incident to other relevant Union and national authorities and shall notify them accordingly. The ECB shall notify the members of the European System of Central Banks on issues relevant to the payment system.

On the basis of that notification, the competent authorities shall, where appropriate, take all of the necessary measures to protect the immediate safety of the financial system.

3 By 13 January 2018, EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, issue guidelines in accordance with Article 16 of Regulation (EU) No 1093/2010 addressed to each of the following:

a payment service providers, on the classification of major incidents referred to in paragraph 1, and on the content, the format, including standard notification templates, and the procedures for notifying such incidents;

b competent authorities, on the criteria on how to assess the relevance of the incident and the details of the incident reports to be shared with other domestic authorities.

4 EBA shall, in close cooperation with the ECB, review the guidelines referred to in paragraph 3 on a regular basis and in any event at least every 2 years.

5 While issuing and reviewing the guidelines referred to in paragraph 3, EBA shall take into account standards and/or specifications developed and published by the European Union Agency for Network and Information Security for sectors pursuing activities other than payment service provision.

6 Member States shall ensure that payment service providers provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide EBA and the ECB with such data in an aggregated form.

Article 97

Authentication

1 Member States shall ensure that a payment service provider applies strong customer authentication where the payer:

a accesses its payment account online;

b initiates an electronic payment transaction;

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

2 With regard to the initiation of electronic payment transactions as referred to in point (b) of paragraph 1, Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

3 With regard to paragraph 1, Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

4 Paragraphs 2 and 3 shall also apply where payments are initiated through a payment initiation service provider. Paragraphs 1 and 3 shall also apply when the information is requested through an account information service provider.

5 Member States shall ensure that the account servicing payment service provider allows the payment initiation service provider and the account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user in accordance with paragraphs 1 and 3 and, where the payment initiation service provider is involved, in accordance with paragraphs 1, 2 and 3.

Article 98

Regulatory technical standards on authentication and communication

1 EBA shall, in close cooperation with the ECB and after consulting all relevant stakeholders, including those in the payment services market, reflecting all interests involved, develop draft regulatory technical standards addressed to payment service providers as set out in Article 1(1) of this Directive in accordance with Article 10 of Regulation (EU) No 1093/2010 specifying:

a the requirements of the strong customer authentication referred to in Article 97(1) and (2);

b the exemptions from the application of Article 97(1), (2) and (3), based on the criteria established in paragraph 3 of this Article;

c the requirements with which security measures have to comply, in accordance with Article 97(3) in order to protect the confidentiality and the integrity of the payment service users' personalised security credentials; and

d the requirements for common and secure open standards of communication for the purpose of identification, authentication, notification, and information, as well as for the implementation of security measures, between account servicing payment service providers, payment initiation service providers, account information service providers, payers, payees and other payment service providers.

2 The draft regulatory technical standards referred to in paragraph 1 shall be developed by EBA in order to:

a ensure an appropriate level of security for payment service users and payment service providers, through the adoption of effective and risk-based requirements;

b ensure the safety of payment service users' funds and personal data;

c secure and maintain fair competition among all payment service providers;

d ensure technology and business-model neutrality;

e allow for the development of user-friendly, accessible and innovative means of payment.

3 The exemptions referred to in point (b) of paragraph 1 shall be based on the following criteria:

a the level of risk involved in the service provided;

b the amount, the recurrence of the transaction, or both;

c the payment channel used for the execution of the transaction.

4 EBA shall submit the draft regulatory technical standards referred to in paragraph 1 to the Commission by 13 January 2017.

Power is delegated to the Commission to adopt those regulatory technical standards in accordance with Articles 10 to 14 of Regulation (EU) No 1093/2010.

5 In accordance with Article 10 of Regulation (EU) No 1093/2010, EBA shall review and, if appropriate, update the regulatory technical standards on a regular basis in order, inter alia, to take account of innovation and technological developments.