STATUTORY INSTRUMENTS

2017 No. 752

The Payment Services Regulations 2017

PART 7

Rights and Obligations in Relation to the Provision of Payment Services

Miscellaneous

Consent for use of personal data

97. A payment service provider must not access, process or retain any personal data for the provision of payment services by it, unless it has the explicit consent of the payment service user to do so.

Management of operational and security risks

98.—(1) Each payment service provider must establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services it provides. As part of that framework, the payment service provider must establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

(2) Each payment service provider must provide to the FCA an updated and comprehensive assessment of the operational and security risks relating to the payment services it provides and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.

(3) Such assessment must—

(a) be provided on an annual basis, or at such shorter intervals as the FCA may direct; and

(b) be provided in such form and manner, and contain such information, as the FCA may direct.

Incident reporting

99.—(1) If a payment service provider becomes aware of a major operational or security incident, the payment service provider must, without undue delay, notify the FCA.

(2) A notification under paragraph (1) must be in such form and manner, and contain such information, as the FCA may direct.

(3) If the incident has or may have an impact on the financial interests of its payment service users, the payment service provider must, 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.

(4) Upon receipt of the notification referred to in paragraph (1), the FCA must—

(a) without undue delay, provide the relevant details of the incident to the European Banking Authority and to the European Central Bank;

(b) notify any other relevant authorities in the United Kingdom; and

(c) co-operate with the European Banking Authority and the European Central Bank in assessing the relevance of the incident to authorities outside of the United Kingdom.

(5) If the FCA receives notification of an incident from the European Banking Authority or the European Central Bank it must take any appropriate measures to protect the immediate safety of the financial system.

Authentication

100.—(1) A payment service provider must apply strong customer authentication where a payment service user—

(a) accesses its payment account online, whether directly or through an account information service provider;

(b) initiates an electronic payment transaction; or

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

(2) Where a payer initiates an electronic remote payment transaction directly or through a payment initiation service provider, the payment service provider must apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.

(3) A payment service provider must maintain adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials.

(4) An account servicing payment service provider must allow a payment initiation service provider or account information service provider to rely on the authentication procedures provided by the account servicing payment service provider to a payment service user in accordance with the preceding paragraphs of this regulation.

(5) Paragraphs (1), (2) and (3) are subject to any exemptions from the requirements in those paragraphs provided for in regulatory technical standards adopted under Article 98 of the payment services directive.

Dispute resolution

101.—(1) This regulation applies in relation to complaints from payment service users who are not eligible within the meaning of section 226(6) of the 2000 Act (the ombudsman scheme – compulsory jurisdiction).

(2) A payment service provider must put in place and apply adequate and effective complaint resolution procedures for the settlement of complaints from payment service users about the rights and obligations arising under Parts 6 and 7.

(3) Those procedures must—

(a) be applied in every EEA State where the payment service provider offers the payment services; and

(b) be available in an official language of each such EEA State, or in another language if agreed between the payment service provider and the payment service user.

(4) When a payment service provider receives a complaint from a payment service user, the payment service provider must make every possible effort to address all points raised in a reply to the complaint on paper or, if agreed between payment service provider and payment service user, in another durable medium.

(5) Subject to paragraph (6), the reply must be provided to the complainant within an adequate timeframe and at the latest 15 business days after the day on which the payment service provider received the complaint.

(6) In exceptional situations, if a full reply cannot be given in accordance with paragraph (4) for reasons beyond the control of the payment service provider, the payment service provider must send a holding reply, clearly indicating the reasons for the delay in providing a full reply to the complaint and specifying the deadline by which the payment service user will receive a full reply.

(7) The deadline specified under paragraph (6) must not be later than 35 business days after the day on which the payment service provider received the complaint.

(8) The payment service provider must inform the payment service user about the details of one or more providers of dispute resolution services able to deal with disputes concerning the rights and obligations arising under this Part and Part 6 (information requirements for payment services), if the payment service provider uses such services.

(9) The payment service provider must also make available in a clear, comprehensive and easily accessible way—

(a) the information referred to in paragraph (7); and

(b) details of how to access further information about any provider of dispute resolution services referred to in paragraph (8) and the conditions for using such services.

(10) The information to be made available under paragraph (8) must be made available—

(a) on the website of the payment service provider (if any);

(b) at branches of the payment service provider (if any); and

(c) in the general terms and conditions of the contract between the payment service provider and the payment service user.