Appendix 2

CONDUCT OF BUSINESS RULEBOOK (COBS)

*In this attachment underlining indicates new text and striking through indicates deleted text.

14. CLIENT MONEY AND RELEVANT MONEY PROVISIONS

...

14.13.4 A pooling event under Rule 14.13.3(c) does not occur when the Authorised Person has notified the Regulator in accordance with Rule 14.11.8 and~~, in~~ the Authorised Person is taking steps, in consultation with the Regulator, to rectify those records and there are reasonable grounds to conclude that the records will be capable of reconciliation within a reasonable period.

...

17.5 Technology Governance and Controls

...

Risk management

(e) A risk management plan containing a detailed analysis of likely risks with both high and low impact, as well as mitigation strategies. The risk management plan must cover, but is not limited to:

(i) operational risks;

(ii) technology risks, including 'hacking' related risks;

(iii) market risk for each Accepted Virtual Asset; and

(iv) risk of Financial Crime.

Guidance

GEN 3.5 contains additional requirements that apply to Authorised Persons in relation to Cyber Risk management.

...

19.23 Risk mitigation and Reporting

Management of operational and security risks

19.23.1 (1) A 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.

(2) 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.

(3) A comprehensive assessment of operational and security risks must be undertaken by the Payment Service Provider relating to the Payment Services it provides, at least annually or more frequently if requested by the Regulator, and provided to the Regulator on request.

(4) The assessment must address the adequacy of the mitigation measures and control mechanisms implemented in response to those risks in such form and manner, and contain such information, as the Regulator may direct.

Guidance

1. The FSRA may require a Payment Service Provider to engage technical experts to generate an audit report addressed to the FSRA, in order to provide independent assurance that the systems and controls employed by the Payment Service Provider comply with the requirements imposed by this Chapter.

2. Payment Service Providers are expected to provide a summary of the information required by Rule 19.23.1 as part of the periodic IRAP assessments undertaken in accordance with PRU 10.3.

3. GEN 3.5 contains additional requirements that apply to Authorised Persons in relation to Cyber Risk management.

Incident reporting

19.23.2 (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 Regulator.

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

Guidance

1. Upon receipt of the notification referred to in 19.23.2(1), the Regulator may notify any other relevant authorities in the U.A.E.

2. If the Regulator receives notification of an incident from any relevant regulator in the U.A.E. or internationally, it may direct the Payment Service Provider to take appropriate measures to protect the immediate safety of their Payment Service Users and the financial system.

3. GEN 3.5.18 and 8.10.6 also require Authorised Persons to notify the Regulator in certain circumstances.

...

20.14 Reporting and Risk mitigation

Management of operational and security risks

20.14.1 (1) A Third Party Provider must establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks relating to the Third Party Services it provides.

(2) As part of that framework, the Third Party Provider must establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

(3) A comprehensive assessment of operational and security risks must be undertaken by the Third Party Provider relating to the Third Party Services it provides, at least annually or more frequently if requested by the Regulator, and provided to the Regulator on request.

(4) The assessment must address the adequacy of the mitigation measures and control mechanisms implemented in response to those risks in such form and manner, and contain such information, as the Regulator may direct.

Guidance

1. The Regulator may provide further guidance to Third Party Providers on their management of technology and data risks that sets out the Regulator's expectations on how Third Party Providers should meet their obligations under this section and other applicable Rules. A Third Party Provider's use of such guidance will be taken into account as part of the ongoing supervisory process of assessing Third Party Providers' risk profile.

2. GEN 3.5 contains additional requirements that apply to Authorised Persons in relation to Cyber Risk management.

Incident reporting

20.14.2 (1) A Third Party Provider must notify the Regulator without undue delay if it becomes aware of a major operational or security incident.

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

(3) The Third Party Provider must inform its Customers without undue delay of the incident and the measures that it will take to mitigate the incident if the incident has or may have an impact on the financial interests of its Customers.

Guidance

1. Upon receipt of the notification referred to in 20.14.2(1), the Regulator may notify any other relevant authorities in the U.A.E.

2. If the Regulator receives notification of an incident from any relevant regulator in the U.A.E. or internationally, it may direct the Third Party Provider to take appropriate measures to protect the immediate safety of their Customers and the financial system.

3. GEN 3.5.18 and 8.10.6 also require Authorised Persons to notify the Regulator in certain circumstances.

...