OPEN BANKING MODULE

MODULE:	OB (Open Banking)

Table of Contents

OB-1.1 Risks, Systems and controls (continued)

OB-1.1.12 A PISP must establish procedures to ensure:

(a) that it will not store a customer's personalised security credentials, such as customer's KYC and biometric information and that such data are:
   i. not accessible to other parties, with the exception of the issuer of the credentials; and
   ii. transmitted through safe and efficient channels;

(b) that any other information about a customer is not provided to any person except a payee, and is provided to the payee only with the customer's explicit consent;

(c) that each time a PISP initiates a payment order on behalf of its customer, the PISP identifies itself to the licensee with whom the customer maintains the account in a secure way;

(d) [This Sub-paragraph was deleted in July 2021];

(e) that it will not access, use or store any information for any purpose except for the provision of a payment initiation service explicitly requested by a payer, however, it may store payment details initiated by the customer such as payment amounts, payment accounts, payment reference number, payment execution dates, time and payee's IBAN number;

(f) that it cannot and does not change the amount, the payee or any other feature of a transaction notified to it by the customer; and

(g) that any data accessed and stored is encrypted in transit and at rest and, must not be accessible to any unauthorised person within the licensee's organisation.

OB-1.1 Risks, Systems and controls (continued)

OB-1.1.13 An AISP must establish procedures to ensure:

(a) it does not provide account information services without the customer's explicit consent;

(b) that it will not store the customer's personalised security credentials such as customer's KYC and biometric information and that such data are:

i. not accessible to other parties, with the exception of the issuer of the credentials; and

ii. transmitted through safe and efficient channels;

(c) for each communication session, communicate securely with licensee and the customer in accordance with the regulatory requirements of this Module;

(d) that it does not access any information other than information from designated accounts;

(e) it will not access, use, or store any information for any purpose except for the provision of the account information service explicitly requested by the customer;

(f) that any data accessed and stored is encrypted in transit and at rest and, must not be accessible to any unauthorised person within the licensee's organisation; and

(g) that customer information accessed must not be stored in a form which permits identification of customer once the customer consent is withdrawn.

MODULE	OB:	Open Banking
CHAPTER	OB-2:	Operating Rules

OB-2.1 Framework Contracts

Legal arrangement and transparency

OB-2.1.1 AISPs and PISPs must establish a framework contract (a legal arrangement) with the customer prior to providing AIS or PIS services. The framework contract must provide the information set forth below that are relevant to the services they provide:

(a) The following information about the service and the provider:

i. the name, address and contact details of the PISP or AISP as the case may be;

ii. a description of the main characteristics of the service to be provided;

iii. the information or unique identifier that must be provided by the customer in order for a payment order to be properly initiated or executed;

(b) the form and procedures for giving consent, to provide account information service, the initiation of a payment order and for the withdrawal of consent;

(c) provisions regarding the time of receipt of a payment order and the cut-off time, if any, established by the licensee and the maximum execution time for the payment services to be provided;

(d) whether spending limits for the use of a payment instrument may be agreed;

(e) the detail of all fees and charges payable by the customer to the PISP/AISP, including those connected to the manner in and frequency with which information is provided or made available and, where applicable, a breakdown of the amounts of any charges;

(f) the means of communication agreed between the parties for the transmission of information or notifications under this Module including, where relevant, any technical requirements for the customer's equipment and software for receipt of the information or notifications;

(g) The terms under which the customer may opt out from the use of the payment instrument;

(h) explicit consents required for generic marketing promotions by the PISP/AISP; and

(i) the terms of the framework contract and information.

OB-2.1 Framework Contracts (continued)

(j) The following information about safeguards and corrective measures in compliance with PDPL:

i. where relevant, a description of the steps that the customer is to take in order to keep safe a payment instrument and how to notify the PISP/AISP for the purposes of obligations of the customer in relation to loss, theft, misappropriation, unauthorised use of the payment instruments and personalised security credentials;

ii. the secure procedures, by which the PISP/AISP will contact the customer in the event of suspected or actual fraud or security threats;

iii. the conditions under which the PISP/AISP stops or prevents the use of a payment instrument;

iv. the customer's liability, (payer or payee's liability for unauthorized payment transactions), including details of any limits on such liability;

v. how and within what period of time the customer is to notify the licensee maintaining customer account of any unauthorised or incorrectly initiated or executed payment transaction, and liability, if any for unauthorised payment transactions falling on the licensee maintaining customer account for execution of unauthorised payment transactions);

vi. liability, if any, in the event of initiation or execution or non-execution or defective or late execution of payment transactions;

vii. liability of parties in the event of a cyber-attack and loss of sensitive data; and

viii. the conditions for any refunds for payment transactions initiated by or through a payee.

OB-2.1 Framework Contracts (continued)

(k) The following information about changes to and termination of the framework contract:

i. the time given to the customer to review and accept any proposed changes; which under no circumstances, shall be less than 10 calendar days;

ii. the proposed terms under which the customer will be deemed to have accepted changes to the framework contract in accordance, unless they notify the service provider that they do not accept such changes before the proposed date of their entry into force;

iii. the duration of the framework contract;

iv. where relevant, the right of the customer to terminate the framework contract and any agreements relating to.

(l) The following information about redress:

i. any contractual clause on the law applicable to the framework contract;

ii. the customer complaint procedures and the availability of alternative dispute resolution procedures for the customer and the methods for having access to them; and

iii. the name/title and contact number of the person designated to handle any queries or complaints.

OB-2.1.2 The information specified in Paragraph OB-2.1.1 must be provided to the customer free of charge before initiation of service.

OB-2.1.3 (a) A framework contract may provide for the PISP to have the right to stop the use of a payment instrument on reasonable ground relating to the security of the payment instrument; or
(b) the suspected unauthorised or fraudulent use of the payment instrument.

OB-2.1 Framework Contracts (continued)

OB-2.1.4 **AISPs and PISPs must agree the basis, the time period and the manner in which the information on its intention to stop the use of the payment instrument will be provided to the customer and to the relevant licensees maintaining customer accounts.**

OB-2.1.5 **AISPs must allow customers to provide consent for accessing their account information for a duration of up to 12 months.**

OB-2.1.6 **AISPs must allow their customers to choose the nature and type of data to be collected or accessed and used by the AISP for the purpose of providing the services.**

OB-2.2 Standards for Authentication and Communication

Secure authentication

OB-2.2.1 **AISPs and PISPs must have in place a 2-factor authentication process to prevent unauthorised access.**
(a) [This Sub-paragraph was deleted in July 2021];
(b) [This Sub-paragraph was deleted in July 2021];
(c) [This Sub-paragraph was deleted in July 2021].

OB-2.2.2 [This Paragraph has been deleted in July 2021].

OB-2.2.3 **[This Paragraph was deleted in July 2021].**
(a) [This Sub-paragraph was deleted in July 2021];
(b) [This Sub-paragraph was deleted in July 2021];
(c) [This Sub-paragraph was deleted in July 2021];
(d) [This Sub-paragraph was deleted in July 2021].

OB-2.2 Standards for Authentication and Communication (continued)

~~*Independence of elements of strong authentication*~~

OB-2.2.4 [This Paragraph was deleted in July 2021].
(a) [This Sub-paragraph was deleted in July 2021];
(b) [This Sub-paragraph was deleted in July 2021]
(c) [This Sub-paragraph was deleted in July 2021].

OB-2.2.5 [This Paragraph was deleted in July 2021].

OB-2.2.6 [This Paragraph was deleted in July 2021].
(a) [This Sub-paragraph was deleted in July 2021];
(b) [This Sub-paragraph was deleted in July 2021].

OB-2.3 Payment Transactions (continued)

Limits on Payment Transactions

OB-2.3.5 The PISP may agree on payment transaction limits based on its own discretion or on account of the following limitations:
(a) limits imposed by the CBB from time to time;
(b) limits imposed by any of the licensees; and/or
(c) limits imposed based on customer request.

OB-2.3.6 Subject to the framework contract, a PISP has the right to stop the use of a payment instrument on reasonable ground relating to:
(a) the security of the payment instrument; or
(b) the suspected unauthorised or fraudulent use of the payment instrument.

OB-2.3.7 PISPs must ensure that a customer to whom a payment instrument has been issued must keep safe the personalised security credentials and must:
(a) use it in accordance with the terms and conditions governing such use; and
(b) notify the PISP in an agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

Fees and charges

OB-2.3.8 The AISPs and PISPs may charge fees and charges which reasonably corresponds to the AISP's or PISP's costs, as the case may be, which must be explicitly agreed in the framework contract.

MODULE	OB:	Open Banking
CHAPTER	OB-2:	Operating Rules

OB-2.4 Technology Related Requirements

OB-2.4.1 AISPs and PIPSs must adhere to the Operational Guidelines, Security Standards and Guidelines, Open Banking Application Program Interface (API) Specifications and Customer Journey Guidelines included in Bahrain Open Banking Framework (See CBB website).

OB-2.4.2 AISPs, PISPs must ensure that compliance with standards and guidelines specified in Paragraph OB-2.4.1 is subject to independent review and tests, including testing in a test environment, by an independent consultant upon implementation.

OB-2.4.3 AISPs and PISPs must ensure that the technology solution provided to their customers is easily accessible and can be downloaded as a standalone application (e.g. IOS/Android/Microsoft Windows etc.).