GENERAL REQUIREMENTS MODULE

CONSULTATION

GR-6.1 Access to PISPs and AISPs

GR-6.1.1 The CBB has recognised the need to revise its rules in keeping with the following changes at a systemic level, both globally and regionally:

a) market growth in e-commerce activities;
b) increased use of internet and mobile payments;
c) consumer demand to increasingly use smart device based payment solutions;
d) the developments in innovative technology; and
e) a trend towards customers having multiple account providers.

This section sets forth the rules applicable to conventional retail bank licensees with regards to the new category of ancillary service providers described below.

GR-6.1.2 The CBB has established a Directive contained in "Module OB: Open Banking" in Volume 5 of the CBB Rulebook that deals with a new sub category of ancillary service providers who, under the terms of the CBB license, may provide "payment initiation services" and/or "account information services". Such licensees are termed "payment initiation service providers" or PISPs and "account information service providers" or AISPs. Banks and other licensees which maintain a customer account is referred to in the CBB Rulebook Volume 5 as "licensees maintaining customer accounts".

GR-6.1.3 **Conventional retail bank licensees must:**

(a) grant ancillary service providers of the types referred to in Paragraph AU-1.2.1 (f) and (g) of Rulebook Volume 5: Ancillary Service Providers Authorisation Module, access to customer accounts on an objective, non-discriminatory basis based on consents obtained from the customer (both natural and legal persons);

(b) provide the criteria that the conventional retail bank licensees apply when considering requests pursuant to sub-paragraph (a) above for such access; and

(c) ensure that those criteria are applied in a manner which ensures compliance with sub-paragraph (a) above while ensuring adherence to Law No 30 of 2018, Personal Data Protection Law (PDPL) issued on 12 July 2018.

GR-6.1.4 **Access to customer accounts granted pursuant to Paragraph GR-6.1.3 must be sufficiently extensive to allow the AISP and PISP access in an unhindered and efficient manner.**

CONSULTATION

GR-6.1 Access to PISPs and AISPs (continued)

GR-6.1.5 Access to customer accounts granted pursuant to Paragraph GR-6.1.3 shall mean that at customer's direction, the licensees are obliged to share without charging a fee, all information that has been provided to them by the customer and that which can be accessed by the customer in a digital form. The obligation should only apply where the licensee keeps that information in a digital form. Furthermore, the obligation should not apply to information supporting identity verification assessment; which the licensees should only be obliged to share with the customer directly, not a data recipient. The information accessed and shared shall include transaction data, relevant Merchant Category Code information and product and services data that banks are required to publicly disclose, such as price, fees, and other charges should be made publicly available under open banking. Fees may be charged by banks to AISPs for sharing 'Value Added Data' and 'Aggregated Data' are not required to be shared. Value added data or derived data results from material enhancement by the application of insights, analysis, or transformation on customer data by the licensee. Aggregated data refers to data which is aggregated across the licensee's customer segments for the purpose of analysis.

GR-6.1.6 **If a conventional retail bank licensee refuses a request for access to such services or withdraws access to such services, it must seek approval of the CBB in a formal communication which must contain the reasons for the refusal or the withdrawal of access and contain such information as the CBB may direct. The CBB shall approve the request if it is satisfied that the impact of not giving access is minimal. If the request is rejected, the conventional retail bank licensee must adhere to the direction provided by the CBB.**

GR-6.1.7 **Conventional retail bank licensees must comply with each of the following requirements:**

(a) provide access to the same information from designated customer accounts made available to the customer when directly requesting access to the account information, provided that this information does not include sensitive payment data (such as customer security credentials or other personalised data, the holding of which or the use of which is not authorised by the customer; and data which may be used by the holder for unauthorised, fraudulent, illegal or activity or transactions);

(b) provide, immediately after receipt of the payment order, the same information on the initiation and execution of the payment transaction provided or made available to the customer when the transaction is initiated directly by the latter;

(c) upon request, immediately provide PISPs with a confirmation whether the amount necessary for the execution of a payment transaction is available on the payment account of the payer. This confirmation must consist of a simple 'yes' or 'no' answer.

CONSULTATION

GR-6.1 Access to PISPs and AISPs (continued)

GR-6.1.8 For the purposes of this Chapter, conventional retail bank licensees must provide access to and share information and data pertaining to customer account activity, including the Merchant Category Code information relevant to the payments from the customer account, and balances of individuals (natural persons) covering a period of 12 full months or 365 days at the time of access to the AISPs in respect of the following services/products offered by the licensee:

(a) Savings accounts;
(b) Current accounts;
(c) Term and call deposits;
(d) Foreign currency accounts;
(e) Unrestricted investment accounts;
(f) Restricted investment accounts;
(g) Mortgage/housing finance products;
(h) Auto loans;
(i) Consumer loans/financing;
(j) Overdrafts (personal);
(k) Credit and charge cards;
(l) Electronic wallets and prepaid cards; and
(m) Other accounts which are accessible to the customer through e-banking portal or mobile device.

GR-6.1.8A For the purposes of Paragraph GR-6.1.7, where conventional retail bank licensees have arrangements to provide access to information and data pertaining to account activity and balances of legal persons, they must provide relevant information covering a period of 12 full months, or 365 days at the time of access, to the AISPs in respect of the following services/products offered by the licensee:

(a) Current and saving accounts;
(b) Overdrafts*;
(c) Term and call deposits;
(d) Foreign currency accounts;
(e) Treasury products;
(f) Unrestricted investment accounts;
(g) Restricted investment accounts;
(h) Financing products*;
(i) Trade finance products*;
(j) Credit and charge cards;
(k) Electronic wallets and prepaid cards; and
(l) Other accounts which are accessible to the customer through e-banking portal or mobile device.

* Including off-balance sheet commitments, guarantees and other lines of credit.

CONSULTATION

GR-6.2 Communication Interface for PISPs and AISPs

GR-6.2.1 Conventional retail bank licensees that offer a customer account that is accessible online must have in place at least one interface which meets each of the following requirements:

(a) AISPs and PISPs must identify themselves in sessions with conventional retail bank licensees;

(b) AISPs and PISPs must communicate securely to request and receive information on one or more designated payment accounts and associated payment transactions; and

(c) PISPs must communicate securely to initiate a payment order from the payer's payment account and receive information on the initiation and the execution of payment transactions.

GR-6.2.2 Conventional retail bank licensees must establish the interface(s) referred to in Paragraph GR-6.2.1 by means of a dedicated interface.

GR-6.2.3 For the purposes of authentication of the customer, the interfaces referred to in paragraph GR-6.2.1 must allow AISPs and PISPs to rely on the authentication procedures provided by the conventional retail bank licensee to the customer. In particular, the interface must meet all of the following requirements:

(a) process for instructing and authentication by the conventional retail bank licensee;

(b) establishing and maintaining authentication of communication sessions between the conventional retail bank licensee, the AISP, the PISP and the customer(s); and

(c) ensuring the integrity and confidentiality of the personalised security credentials and of authentication codes transmitted by or through the AISP or the PISP.

GR-6.2.4 Conventional retail bank licensees must ensure that their interface(s) follows standards of communication which are agreed by the CBB and that the protocols are technology neutral. They must ensure that the technical specifications of the interface are documented and are made available to AISPs and PISPs when requested.

CONSULTATION

GR-6.2 Communication Interface for PISPs and AISPs (continued)

GR-6.2.5 Conventional retail bank licensees must establish and make available a testing facility, in accordance with the operational guidelines included in the Bahrain Open Banking Framework (see Section 4.1) to authorised AISPs and PISPs, companies operating in the CBB's Regulatory Sandbox as open banking service providers and AISPs/PISPs granted in-principle confirmation to proceed with the CBB's licensing process. No sensitive information must be shared through the testing facility. Licensees must display a link to the testing facility on their website.

GR-6.2.6 Conventional retail bank licensees must ensure that the dedicated interface established for the AISPs and PISPs offers the same level of availability and performance, including support, as well as the same level of contingency measures, as the interface made available to the customer for directly accessing its payment account online.

GR-6.2.7 For the purposes of GR-6.2.6, the following requirements apply:

(a) conventional retail bank licensees must monitor the availability and performance of the dedicated interface and make the resulting statistics available to the CBB upon their request;

(b) where the dedicated interface does not operate at the same level of availability and performance as the interface made available to the conventional retail bank licensee's customer when accessing the payment account online, the bank must report it to the CBB and must restore the level of service for the dedicated interface without undue delay and take the necessary action to avoid its reoccurrence;

(c) the report referred to in (b) above must include the causes of the deficiency and the measures adopted to re-establish the required level of service; and

(d) AISPs and PISPs making use of the dedicated interface offered by conventional retail bank licensees must also report to the CBB any deficiency in the level of availability and performance required of the dedicated interface.

GR-6.2.8 Conventional retail bank licensees must include in the design of dedicated interface, a strategy and plans for contingency measures in the event of an unplanned unavailability of the interface and systems breakdown. The strategy must include communication plan to inform the relevant AISP/PISP making use of the dedicated interface in the case of breakdown, measures to bring the system back to 'business as usual' and a description of alternative options AISPs and PISPs may make use of during the unplanned downtime.

CONSULTATION

GR-6.3 Security of Communication Sessions and Authentication

GR-6.3.1 Conventional retail bank licensees must ensure that communication sessions with PISPs and AISPs including merchants, relies on each of the following:

(a) a unique identifier of the session;

(b) security mechanisms for the detailed logging of the transaction, including transaction number, timestamps and all relevant transaction data;

(c) timestamps which must be based on a unified time-reference system and which must be synchronised according to an official time signal.

GR-6.3.2 Conventional retail bank licensees must ensure secured identification when communicating with AISPs and PISPs.

GR-6.3.3 Conventional retail bank licensees must ensure that, when exchanging data via the internet, with PISPs and AISPs, secure encryption is applied between the communicating parties throughout the respective communication session in order to safeguard the confidentiality and the integrity of the data, using strong and widely recognised encryption techniques.

GR-6.3.4 PISPs and AISPs must keep the access sessions offered by conventional retail bank licensees as short as possible and they must actively terminate the session as soon as the requested action has been completed.

GR-6.3.5 When maintaining parallel network sessions with the PISPs and AISPs, conventional retail bank licensees must ensure that those sessions are securely linked to relevant sessions established in order to prevent the possibility that any message or information communicated between them could be misrouted.

CONSULTATION

GR-6.3 Security of Communication Sessions and Authentication (continued)

GR-6.3.6 Conventional retail bank licensees' sessions with PISPs and AISPs must contain unambiguous reference to each of the following items:

(a) the customer and the corresponding communication session in order to distinguish several requests from the same customer;

(b) for payment initiation services, the uniquely identified payment transaction initiated.;

(c) for confirmation on the availability of funds, the uniquely identified request related to the amount necessary for the execution of the transaction.

GR-6.3.7 Conventional retail bank licensees must ensure that where they communicate personalised security credentials and authentication codes, these are not readable by any staff at any time.

GR-6.3.8 [This Paragraph was moved to GR-6.1.7].

CONSULTATION

GR-6.3 Security of Communication Sessions and Authentication (continued)

GR-6.3.9 In case of an unexpected event or error occurring during the process of identification, authentication, or the exchange of the data elements, the conventional retail bank licensees must send a notification message to the relevant PISP or AISP which explains the reason for the unexpected event or error.

GR-6.3.10 Where the conventional retail bank licensee offers a dedicated interface, it must ensure that the interface provides for notification messages concerning unexpected events or errors to be communicated by any PISP or AISP that detects the event or error to the other licensees participating in the communication session.

GR-6.3.11 Conventional retail bank licensees must provide access to information from customer accounts to AISPs whenever the customer requests such information.

Secure authentication

GR-6.3.12 Conventional retail bank licensees must have in place a strong customer authentication process and ensure the following:

(a) no information on any of the elements of the strong customer authentication 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 code previously generated; and

(c) the authentication code cannot be forged.

GR-6.3.13 Conventional retail bank licensees must adopt security measures that meet the following requirements for payment transactions:

(a) the authentication code generated must be specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;

(b) the authentication code accepted by the licensee maintaining customer account corresponds to the original specific amount of the payment transaction and to the payee agreed to by the payer;

(c) a SMS message must be sent to the customer (in the case of customers who are natural persons) upon accessing the online portal or application and when a transaction is initiated; and

(d) any change to the amount or the payee must result in the invalidation of the authentication code generated.

CONSULTATION

GR-6.3 Security of Communication Sessions and Authentication (continued)

Independence of elements of strong authentication

GR-6.3.14 Conventional retail bank licensees must establish adequate security features for customer authentication including the use of the following three elements:

(a) an element categorised as knowledge (something only the user knows), such as length or complexity of the pin or password;

(b) an element categorised as possession (something only the user possesses) such as algorithm specifications, key length and information entropy, and

(c) for the devices and software that read, elements categorised as inherence (something the user is), i.e. algorithm specifications, biometric sensor and template protection features.

GR-6.3.15 Conventional retail bank licensees must ensure that the elements referred to in Paragraph GR-6.3.14 are independent, so that the breach of one does not compromise the reliability of the others, in particular, when any of these elements are used through a multi-purpose device, i.e. a device such as a tablet or a mobile phone which can be used for both giving the instruction to make the payment and for being used in the authentication process. The CBB will consider exempting from a 3 factor authentication on a case to case basis provided that the licensee is able to demonstrate to CBB that it has established robust controls to mitigate the relevant key risks.

CONSULTATION

GR-6.4 Standards for Program Interfaces and Communication

GR-6.4.1 Conventional retail bank licensees 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, "BOBF" (see CBB website) for the use cases defined in the BOBF. Where licensees have arrangements to share customer account information or allow for payment initiation services with AISPs/PISPs for use cases not defined in BOBF, they must ensure that the API Specifications, Customer Journeys and Operational Guidelines are consistent with the Security Standards and Guidelines in BOBF.

GR-6.4.1A Conventional retail bank licensees, when sharing account information or for payment initiation services related to legal persons, must agree the API Specifications, Customer Journeys and Operational Guidelines with the relevant AISP/PISP and the legal person. The arrangements in this respect must consider the rights, obligations and accountability of all parties, including, but not limited to, conditions relating to customer consents, authentication, authorisation, errors or omissions, downtime, fraud, data security and confidentiality and dispute resolution.

GR-6.4.2 Conventional retail bank licensees must ensure that compliance with standards and guidelines specified in Paragraph GR-6.4.1 is subject to independent review and tests, including testing in a test environment., by an independent consultant upon implementation.

GR-6.4.3 To remain technologically neutral the technical standards adopted by conventional retail bank licensees must not require a specific technology to be adopted by AISPs or PISPs. Authentication codes must be based on solutions such as generating and validating one-time passwords, digital signatures or other cryptographically underpinned validity assertions using keys and/or cryptographic material stored in the authentication elements, as long as the security requirements are fulfilled.

CONSULTATION