PAYMENT SERVICE REQUIREMENTS MODULE

MODULE	Payment Service Requirements
CHAPTER	Table of Contents

MODULE	Payment Service Requirements
CHAPTER	Table of Contents

PS-A.1 Purpose

Executive Summary

PS-A.1.1 This Module sets out requirements applicable to licensees that undertake a regulated payment services described in more detail in PS-1 also referred to as PSPs.

PS-A.1.2 The Module establishes a proportionate and tailored approach to regulating and supervising payment service providers (PSPs) business models driven by innovative technology within the digital ecosystem in the Kingdom of Bahrain.

PS-A.1.3 This Module should be read in conjunction with the requirements in other parts of the CBB Rulebook, particularly:

(a) Fit and Proper Requirements Module (Module FP);
(b) Principles of Business Module (Module PB);
(c) High Level Controls Module (Module HC);
(d) General Requirements Module (Module GR);
(e) CBB Reporting Requirements Module (Module BR);
(f) Public Disclosure Module (Module PD);
(g) Auditors and Accounting Standards Module (Module AU);
(h) Financial Crime Module (Module FC); and
(i) Enforcement Module (Module EN).

Legal Basis

PS-A.1.4 This Module contains the CBB's Directive (as amended from time to time) applicable to payment service provider (PSP) licensees and is issued under the powers available to the CBB under Article 38 of the CBB Law.

PS-A.2 Module History

Evolution of Module

PS-A.2.1 This Module was first issued in [Month] 2026. All subsequent changes to this Module are annotated with the month in which the change was made.

PS-A.2.2 A list of recent changes made to this Module is provided below:

Module Ref.	Change Date	Description of Changes

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.1 Licensing

PS-1.1.1 **No person may:**

(a) Undertake (or hold themselves out to undertake) any of the regulated payment services, by way of business, within or from the Kingdom of Bahrain unless duly licensed by the CBB;

(b) Hold themselves out to be licensed by the CBB unless they have as a matter of fact been so licensed; or

(c) Market any regulated payment service in the Kingdom of Bahrain unless:

a. Allowed to do by the terms of a license issued by the CBB;

b. The activities come within the terms of exempt payment services; or

c. Has obtained the express written permission of the CBB to offer financial services.

PS-1.1.2 A person, other than a licensee or an exempt payment service provider, whether in the Kingdom of Bahrain or elsewhere, or a person in the Kingdom on behalf of a person outside the Kingdom, is undertaking a regulated payment service by way of business, if for example, the person concerned:

(a) Is incorporated in the Kingdom of Bahrain;

(b) Uses an address situated in the Kingdom of Bahrain for its correspondence; or

(c) Directly solicits clients, i.e.:

i. offers to provide, or issue any advertisement containing any offer to provide, to the public in the Kingdom or any section of the public in the Kingdom, any type of payment service; or

ii. makes an offer or invitation, or issue any advertisement containing any offer or invitation, to the public in the Kingdom or any section of the public in the Kingdom, to enter into any agreement relating to the provision by any person of any type of payment service.

PS-1.1.3 **Regulated payment services include one or more of the following (refer to appendix PS-1 for definitions):**

(a) Issuance of payment accounts and instruments;

(b) Domestic money transfer;

(c) Cross-border money transfer;

(d) Merchant acquisition;

(e) Crypto-asset based payments;

(f) E-money issuance;

(g) Money-changing;

(h) Payment initiation service; and

(i) Account information service.

PS-1.1 Licensing (continued)

PS-1.1.4 The following services are not regulated payment services:

(a) the service of executing a payment transaction on behalf of the payer or the payee, if performed by a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee, as the case may be;

(b) the service of executing a payment transaction based on any of these documents, each being a document drawn on a person with a view to placing money at the disposal of the payee: any cheque, cashier's order, drawing voucher, dividend warrant, demand draft, remittance receipt, traveller's cheque or gift cheque;

(c) where a person in the Kingdom of Bahrain utilises a PSP in another jurisdiction for the purpose of payments to a merchant or service provider in that jurisdiction;

(d) the service of executing any payment transaction within a payment system or securities settlement system between any 2 or more participants of the system (each being a PSP, settlement agent, central counterparty, clearing house, central bank or any other participant of the system);

(e) the service of executing payment transactions (including both domestic money transfers and cross-border money transfers) between 2 or more related corporations, in any case where the payment transaction is not executed through a PSP or is executed through a PSP that is one of those related corporations;

(f) the service of transporting currency, including the collection, processing and delivery of the currency, even where the provision of the service is carried on by way of business;

(g) any service, including (but not limited to) any of the following services, provided by any technical service provider that supports the provision of any payment service, but does not at any time enter into possession of any money under that payment service:

i. the service of processing and storing data;
ii. any information technology security, trust or privacy protection service;
iii. any data and entity authentication service;
iv. any information technology service;
v. the service of providing a communication network;
vi. the service of providing and maintaining any terminal or device used for any payment service;

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.1 Licensing (continued)

(h) any payment service that is provided by any person in respect of only limited purpose e-money (refer to appendix PS-1 for definition);
(i) any payment service provided by the CBB; and
(j) any crypto-asset based payment service that is provided in respect of only limited purpose tokens (refer to appendix PS-1 for definition).

PS-1.1.5 **A person that wishes to carry on a business of providing any type of regulated payment service must submit an application for a payment service provider license to the CBB. The application for a license must be in the form prescribed by the CBB (Form 1) and must contain:**

(a) A business plan specifying the type of business to be conducted;
(b) Application forms (Form 2) for all controllers; and
(c) Application forms (Form 3) for directors and senior management functions as specified in Module FP of the CBB Rulebook, Common Volume.

PS-1.1.6 **Licensees must seek the CBB's approval for a variation of its license by changing the types of regulated payment services that the license entitles the licensee to carry on.**

PS-1.1.7 **Licensees must submit an application for license, together with the following:**

(a) the identity of the applicant's controllers;
(b) the identity of directors and other persons responsible for the management of the applicant;
(c) the applicant's legal status and articles of association;
(d) an overview of other jurisdictions where the applicant is operating, or submitting or is planning to submit an application for authorisation to operate as a payment service provider;
(e) a programme of operations setting out in particular the type of payment services envisaged;
(f) a business plan including:
i. description of products and services;
ii. revenue and pricing structure;
iii. distribution channels;
iv. target market and customer segments;
v. a forecast budget calculation for the first 3 financial years which demonstrates that the applicant is able to employ the appropriate and proportionate systems, resources and procedures to operate soundly;

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.1 Licensing (continued)

(g) evidence that the applicant holds the minimum base capital;
(h) a description of the measures for safeguarding client money;
(i) a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures, and a description of the applicant's arrangements for the use of IT systems;
(j) a description of the procedure in place to monitor, handle and follow up cyber security incidents and fraud related customer complaints;
(k) a description of business continuity arrangements including a clear identification of the critical operations;
(l) an information security policy document, including:
  i. a detailed risk assessment in relation to the applicant's payment services; and
  ii. a description of controls and mitigation measures to adequately protect payment service users against the risks identified, including fraud and the illegal use of sensitive and personal data;
(m) a description of the internal control mechanisms to comply with the AML Law and CBB's Financial Crime Module;
(n) a description of outsourcing arrangements;
(o) whether the applicant intends to participate in a Bahraini or international payment system/scheme;
(p) the identity of auditors; and
(q) a winding-up plan in case of failure, which is adapted to the envisaged size and business model of the applicant.

PS-1.1.8 The applicant must meet the following conditions for the granting of payment service license:
(a) the applicant has a registered office in the Kingdom of Bahrain or it is incorporated outside the Kingdom;
(b) the applicant satisfies financial requirements prescribed in this Module;
(c) the CBB is satisfied:
  i. that the controllers and ultimate beneficial owners of the applicant are fit and proper;
  ii. as to the financial condition of the applicant;
  iii. that there will be no harm to public interests by the granting of the license;

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.1 Licensing (continued)

(d) the applicant satisfies such operational requirements as the CBB may specify;
(e) the application is accompanied by the required information (Paragraph PS-1.1.9); and
(f) the license application fee is paid.

PS-1.1.9 **Within 60 calendar days of receipt of a license application and submission all the required information, the CBB will inform the applicant whether the license is granted or refused. The CBB will give reasons where it refuses a license application.**

PS-1.1.10 The CBB may impose certain requirements, restrict, suspend or revoke the license where the licensee fails to meet its ongoing obligations. The CBB will only undertake any of the said actions proportionate to the violation of the licensee, details of which are prescribed in the Enforcement Module.

License Fees

PS-1.1.11 **Applicants seeking a PSP license from the CBB must pay a non-refundable license application fee of BD 100 at the time of submitting their formal application to the CBB.**

PS-1.1.12 **PSPs must pay a flat fee of BD 150 to add an activity to its license which was not authorised for previously.**

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.1 Licensing (continued)

PS-1.1.13 The variable annual license fee payable by licensees is 0.25% of their total operating expenses as recorded in the most recent audited financial statements available excluding the items listed below, subject to a minimum ('floor') of BD 2,000 and a maximum ('cap') of BD 24,000:

(a) Training costs;
(b) Charitable donations;
(c) CBB fees paid; and
(d) Non-executive Directors' remuneration.

PS-1.1.14 For new licensees, the variable annual license fee payable must be calculated on the minimum ('floor') of BD 2,000 on a pro-rata basis from the month of obtaining the license.

Voluntary Surrender of a License

PS-1.1.15 In accordance with Article 50 of the CBB Law, a licensee intending to cease carrying out all the approved regulated services, must obtain the CBB's written approval, before ceasing business. All such requests must be made in writing to the Director, Payments Supervision, setting out in full the reasons for the request and how the business is to be wound up.

PS-1.1.16 PSPs must satisfy the CBB that their clients' interests are to be safeguarded during and after the proposed cancellation.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.1 Licensing (continued)

Cancellation of a License by the CBB

PS-1.1.17 Pursuant to Article 48 (c) of the CBB Law, the CBB may cancel a license, for instance if a PSP fails to satisfy any of its existing license conditions or in order to protect the legitimate interests of clients or creditors of the licensee. The CBB generally views the cancellation of a license as appropriate only in the most serious of circumstances and generally tries to address supervisory concerns through other means beforehand.

PS-1.1.18 The procedures for cancellation of a license are contained in Articles 48 and 49 of the CBB Law.

PS-1.1.19 The CBB will only effect the cancellation once a PSP has discharged all its regulatory responsibilities to clients. Until such time, the CBB will retain all its regulatory powers towards the licensee and will direct the PSP so that no new regulated service offering may be undertaken whilst the licensee discharges its obligations to its clients.

Amendment to the Scope of Regulated Services Under the License or Amendment of the License

PS-1.1.20 **PSPs wishing to vary the scope of the regulated services under their existing license, whether by adding or ceasing some services, must obtain CBB's prior written approval.**

Publication of the Decision to Voluntarily Surrender, Cancel or Amend a License

PS-1.1.21 In accordance with Articles 47 and 49 of the CBB Law, the CBB must publish its decision to voluntarily surrender, cancel or amend a license in the Official Gazette and in two local newspapers, one in Arabic and the other in English.

PS-1.1.22 **For the purposes of Paragraph PS-1.1.25, the cost of publication must be borne by the licensee.**

PS-1.1.23 The CBB may also publish its decision on such cancellation or amendment using any other means it considers appropriate, including electronic means.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.2 Financial Resources Requirements

PS-1.2.1 **Licensees must meet the minimum base capital requirements as follows:**

	Activity type	BD
A	Account information	30,000
B	Payment initiation	
C	Issuance of payment account /instruments	50,000
D	Money-changing	
E	Domestic transfer	
F	Cross border transfer	
G	E-money issuance	
H	Cryptoassets based payments	
I	Merchant acquisition	

PS-1.2.2 **Notwithstanding the minimum capital requirements in Paragraph PS-1.2.1, licensees must additionally ensure that the net shareholders' equity is adequate to cover 6 months operating expenses as per the previous year's audited financial statements and, in the case of new licensees, as per the projected financial statements. Operating expenses for this purpose exclude the following items:**

(a) depreciation and amortisation expenses as stated in the financial statements; and

(b) expense items that are not incurred from the ordinary activities and are not expected to recur frequently or regularly. This may include costs from one-time events such as write-offs, purchases of or losses from the sale of the fixed assets, or extraordinary events such as earthquakes or other natural disasters.

PS-1.2.3 Licensees should have policies and systems in place to ensure adherence to the requirements in Paragraphs PS-1.2.1 and PS1.2.2 above. To ensure adherence to these requirements, it is important the licensees have a good estimate of the operating expenses for the foreseeable future to avoid having to increase capital every other year should the scale of operations grow at a rapid pace.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.3 General Requirements

Controller Requirements

PS-1.3.1 Controllers must meet the fit and proper criteria below:

(a) Has not previously been convicted of any felony or crime related to honesty and/or integrity unless subsequently restored to good standing;

(b) Was not the subject of civil or criminal proceedings or enforcement action, in relation to the management of an entity, or commercial or professional activities, which were determined adversely to the person and which reflected adversely on the person's diligence, judgment, honesty or integrity;

(c) Has not been an officer found liable for an offence committed by a body corporate where the offense was proven to have been committed with the consent, connivance, or neglect attributable to that officer;

(d) Has not been refused the right or had restrictions placed on the individual's right to carry on any trade, business, or profession requiring a specific license, registration, or other authorisation by law in any jurisdiction;

(e) Has not been disqualified by a court, regulator, or other competent body from acting as a board director, manager or employee of a company in any jurisdiction;

(f) Has not been reprimanded, or disqualified, or removed by a professional or regulatory body in relation to matters relating to the person's honesty, integrity or business conduct; or

(g) Possesses the qualifications and experience relevant to the regulated activity.

Mind and Management

PS-1.3.2 Licensees must adhere to the Fit and Proper Module for the appointment Board and senior management.

Operational Risk

PS-1.3.3 Licensees must comply with the outsourcing and information security requirements stipulated in Chapters GR-11 and GR-12 of CBB Rulebook Volume 5, Type 7 Ancillary Service Providers.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.3 General Requirements (Continued)

Auditing Requirements

PS-1.3.4 **PSPs must appoint an independent external auditor for every financial year. While appointing an auditor, PSPs must exercise due skill, care and diligence in the selection and appointment of the auditor and must take into consideration the auditor's experience and track record of auditing payment services related businesses. The licensee must pay the fees of the auditor regardless of the manner in which the auditor is appointed.**

PS-1.3.5 In accordance with Article 61(b) of the CBB Law, if a licensee fails to appoint an auditor within four months from the beginning of its financial year, the CBB shall appoint an auditor on behalf of the licensee.

PS-1.3.6 **The CBB may, if it is not satisfied with the performance of any duty by the auditor of a licensee, at any time direct the licensee to remove the auditor and appoint another auditor.**

Complaints Handling

PS-1.3.7 **Licensees must comply with the customer complaints handling procedures stipulated in Chapter GR-10 of CBB Rulebook Volume 5, Type 7 Ancillary Service Providers.**

Regulatory Reporting

PS-1.3.8 **Licensees must comply with the reporting requirements in Appendix PS-2.**

Account Limits

PS-1.3.9 **A PSP that carries on a business of providing an account issuance service must ensure that the e-money contained in a personal payment account issued by the PSP to a natural person does not exceed the amount of BD 10,000 (or its equivalent in a foreign currency) at any point in time. There is no mandated account limit for corporate customers, licensees may set up internal limits based on their risk assessments.**

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.3 General Requirements (continued)

Other General Requirements

PS-1.3.10 Licensees must have at least one person available during working hours to address any queries or complaints from any payment service user that uses any payment service provided by the licensee or is a customer of the licensee.

PS-1.3.11 Licensees must keep, or cause to be kept, books of all the licensee's transactions in relation to any payment service provided by the licensee.

PS-1.3.12 Licensees must notify the CBB for opening a new place of business, closing a place of business or any change in the address of its existing places of business in the Kingdom of Bahrain.

PS-1.3.13 Licensees must notify the CBB of the occurrence of any of the following events as soon as practicable after that occurrence:

(a) any civil or criminal proceeding instituted against the licensee, whether in Bahrain or elsewhere;

(b) any event (including an irregularity in the operations of the licensee) that materially impedes or impairs the operations of the licensee;

(c) the licensee being or becoming, or being likely to become, insolvent or unable to meet any of the licensee's financial, statutory, contractual or other obligations;

(d) any disciplinary action taken against the licensee by any regulatory authority (other than the CBB), whether in Bahrain or elsewhere; and

(e) any significant change to the regulatory requirements imposed on the licensee by any regulatory authority (other than the CBB), whether in Bahrain or elsewhere.

PS-1.3.14 Licensees must not provide any type of payment service in Bahrain through an agent, unless the agent has in force a license that entitles the agent to carry on a business of providing that type of payment service, the agent is an exempt payment service provider in respect of that type of payment service or CBB's approval is given for such arrangements.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.4 Licensing Conditions

Condition 1: Legal Status

PS-1.4.1 **A payment service provider licensee must take one of the following legal forms:**

a) A Bahraini Shareholding Company (B.S.C.); or

b) A With Limited Liability Company (W.L.L.).

Condition 2: Mind and Management

PS-1.4.2 **Licensees must maintain their head office and management in the Kingdom.**

Condition 3: Controllers

PS-1.4.3 **Licensees must satisfy the CBB that their controllers are suitable and pose no undue risks to the licensee. Licensees must also satisfy the CBB that their group structures do not prevent the effective supervision of the licensee by the CBB and otherwise pose no undue risks to the licensee.**

PS-1.4.4 Chapter GR-7 contains the CBB's requirements and definitions regarding controllers.

PS-1.4.5 In summary, controllers are persons who directly or indirectly are significant shareholders in a licensee, or who are otherwise able to exert significant influence on the licensee. The CBB seeks to ensure that controllers pose no significant risks to the licensee. In general terms, controllers are assessed in terms of their financial standing, their judicial and regulatory record, and standards of business and (where relevant) personal probity.

PS-1.4.6 As regards group structures, the CBB seeks to ensure that these do not prevent adequate consolidated supervision being applied to financial entities within the group, and that other group entities do not pose any material financial, reputational or other risks to the licensee.

PS-1.4.7 In all cases, when judging applications from existing groups, the CBB will have regard to the reputation and financial standing of the group as a whole. Where relevant, the CBB will also take into account the extent and quality of supervision applied to overseas members of the group and take into account any information provided by other supervisors in relation to any member of the group.

PS-1.4 Licensing Conditions (Continued)

Condition 4: Board and Employees

PS-1.4.8 Those nominated to the Board or to carry out senior management functions must satisfy the CBB's requirements set out in Module FP of the CBB Rulebook, Common Volume. This rule is supported by Article 65 of the CBB Law.

PS-1.4.9 The licensee's staff, taken together, must collectively provide a sufficient range of skills and experience to manage the affairs of the licensee in a sound and prudent manner. Licensees must ensure their employees meet any training and competency requirements specified by the CBB in Module FP of the CBB Rulebook, Common Volume.

Condition 5: Financial Resources

Capital Funds

PS-1.4.10 Licensees must maintain a level of financial resources, as agreed with the CBB, adequate for the level of business proposed. A greater amount of capital than specified in this Section may be required by the CBB on a case-by-case basis.

Liquidity

PS-1.4.11 Licensees must maintain sufficient liquid assets to meet their obligations as they fall due in the normal course of their business.

Condition 6: Systems and Controls

PS-1.4.12 Licensees must maintain systems and controls that are, in the opinion of the CBB, adequate for the scale and complexity of their activities. These systems and controls must meet the minimum requirements contained in Modules HC and RM (to be issued at a later date).

PS-1.4.13 Licensees must maintain systems and controls that are, in the opinion of the CBB, adequate to address the risks of financial crime occurring in the licensee.

PS-1.4 Licensing Conditions (Continued)

Condition 7: External Auditor

PS-1.4.14 Article 61 of the CBB Law requires that licensees appoint an external auditor, subject to the CBB's prior approval. The minimum requirements regarding auditors contained in Module AA (Auditors and Accounting Standards) must be met.

Condition 8: Other Requirements

Books and Records

PS-1.4.15 Article 59 of the CBB Law requires that licensees must maintain comprehensive books of accounts and other records and satisfy the minimum record-keeping requirements contained in Article 60 of the pre-mentioned Law and Module GR. Books of accounts must comply with the financial accounting standards issued by the International Financial Reporting Standards (IFRS)/International Accounting Standards (IAS) or the applicable AAOIFI standards for Islamic licensees.

Provision of Information

PS-1.4.16 Articles 58, 111, 114 and 163 of the CBB Law require that licensees and their staff must act in an open and cooperative manner with the CBB. Licensees must meet the regulatory reporting and disclosure requirements contained in Module BR. As per Article 62 of the CBB Law, audited financial statements must be submitted to the CBB within 3 months of the licensee's financial year-end.

General Conduct

PS-1.4.17 Licensees must conduct their activities in a professional and orderly manner, in keeping with good market practice. Licensees must comply with the general standards of business conduct contained in Modules PB and GR.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-1:	Licensing Requirements

PS-1.4 Licensing Conditions (Continued)

Additional Conditions

PS-1.4.18 **Licensees must comply with any other specific requirements or restrictions imposed by the CBB on the scope of their license.**

PS-1.4.19 Licensees are subject to the provisions of the CBB Law. These include the right of the CBB to impose such terms and conditions, as it may deem necessary when issuing a license, as specified in Article 45 of the CBB Law. Thus, when granting a license, the CBB specifies the regulated ancillary services that the licensee may undertake. Licensees must respect the scope of their license.

PS-1.4.20 In addition, the CBB may impose additional restrictions or requirements, beyond those already specified in Volume 5, to address specific risks. For instance, a license may be granted subject to strict limitations on intra-group transactions.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-2:	Safeguarding Client Money

PS-2.1 Safeguarding Requirements

PS-2.1.1 This Chapter is applicable to all PSPs that receive client money during the course of providing payment services. PSPs that offer solely account issuance service (i.e. not combined with any other payment service such as e-money issuance), account information services and payment initiation service that do not hold client money will not be subject to this Chapter.

PS-2.1.2 Licensees must ensure that any client money received from, or on behalf of, a customer is deposited into a segregated account with a retail bank, no later than the next business day. Such funds must not be commingled with any other operational account. Client money comprises any money that a licensee holds on a fiduciary basis, as intermediary in the course of carrying on regulated services, towards the execution of transactions on behalf of its customers.

PS-2.1.3 The client money must be safeguarded in one of the following methods:

(a) By depositing the relevant money in a trust account with a retail bank;

(b) Insurance from a regulated insurance firm which is fully liable to the customer for the client money; or

(c) A guarantee given by a retail bank for the amount of the client money.

In the case of cross-border operations, the PSPs must place client money attributable to the overseas operations in a bank rated AA- or above.

PS-2.1.4 Where a PSP chooses to safeguard client money using a guarantee from a bank or an insurance policy from an insurance firm, it must meet the following:

(a) Before obtaining a guarantee or insurance cover from the bank or insurance firm:

i. Assess, and satisfy itself of, the suitability of the bank or insurance firm as the case may be with respect to the giving of the guarantee or providing the insurance cover; and

ii. Give written notice to the bank or insurance firm and obtain an acknowledgment that the guarantee or insurance cover is being obtained by the PSP for the purpose of complying with Paragraph 2.1.3;

PS-2.1 Safeguarding Requirements (continued)

(b) Ensure that:

i. The guarantee states that in the event of the insolvency of the PSP, the bank assumes a primary liability to pay a sum equal to the amount of the client money held by the PSP at the end of the business day immediately preceding the date the PSP becomes insolvent and in case of an insurance cover it is considered claimed at the point of insolvency of the PSP; and

ii. There is no other condition or restriction on the immediate paying out of money by the bank or insurance firm to a separate account held by the PSP, in the event of the insolvency of PSP;

(c) Disclose in writing to the customer that the client money is being safeguarded by a guarantee or insurance cover given by the bank or insurance firm for the client money;

(d) Assess, and satisfy itself of, the suitability of the bank or the insurance firm, as the case maybe, on an annual basis subsequent to obtaining the guarantee or insurance; and

(e) PSPs must retain adequate records in relation to the basis on which the PSP satisfied itself of the suitability of the bank or insurance firm for at least five years.

PS-2.1.5 A licensee must inform the CBB in advance of any material change in measures taken for safeguarding client money.

Contractual Arrangements

PS-2.1.6 An agreement must be established between the PSP and the bank holding the client money. This contract should clearly define the roles, responsibilities, and limitations of both parties regarding the handling of client money.

Controls and Restrictions

PS-2.1.7 Licensees must ensure that it has established and implemented adequate policies, procedures and systems for compliance with client money safeguarding requirements, including but not limited to those related to prevention of misuse and fraud. Licensees must ensure that the client money is reported as a separate balance sheet item in the licensee's financial statements specifying also the nature and purpose for which such funds are held on behalf of its customers.

PS-2.1 Safeguarding Requirements (continued)

PS-2.1.8 For the purposes of PS-2.1.6, controls and restrictions may include but are not limited to the following:

(a) Each payment channel (e.g., E-Commerce, Fawri, Apple Pay, kiosks) should have a dedicated sub-account;
(b) Follow pre-approved methods and channels (no ad-hoc or manual fund movements allowed);
(c) Payment user customers should be whitelisted;
(d) Fund flows should be rule-based, API driven, end user traceability;
(e) Payments should be initiated by the customer;
(f) Only automated, agreed-upon modes of transfer are permitted;
(g) Fund transfers should include purpose codes for classification and compliance;
(h) Suspicious transaction monitoring: systems must flag unusual or suspicious activity;
(i) PSPs must perform daily reconciliations of all accounts and transactions;
(j) Settlements should be made on a gross basis; and
(k) PSPs should not place a lien or pledge on the segregated funds.

PS-2.1.9 A licensee must comply with the following requirements with respect to the safeguarding and management of client money:

(a) Maintain adequate segregation of duties in relation to the operation of client money accounts;
(b) Establish and maintain internal controls and systems to ensure the daily reconciliation of client money balances held with the bank against the corresponding client ledgers; and
(c) Designate a member of senior management as the responsible person for the oversight and operation of client money accounts.

PS-2.1.10 Licensees holding client money in the course of carrying out payment services must appoint independent auditors to perform an audit of client money every 6 months and submit the report to the CBB as required in Paragraph BR-1.1.6.

PS-2.2 Additional Requirements for PSPs Offering Crypto-Asset Based Payment Services

PS-2.2.1 In case of crypto-asset based payments, where the PSP has chosen to safeguard client money by holding it under fiduciary arrangement and the client money is kept in the form of crypto-assets, the said assets must be maintained with a licensed crypto-asset custodian. The CBB may allow self-custody on a case-by-case basis. Where the PSP is allowed to undertake self-custody of the crypto-assets such fact must be disclosed to the customer along with the following:

(a) whether or not the assets will be commingled with assets belonging to other customers of the licensee;

(b) if the assets will be so commingled, the risks arising from such commingling;

(c) the terms and conditions that would apply to the licensee's safeguarding of the assets; and

(d) the consequences for the customer in respect of the assets if the licensee becomes insolvent.

PS-2.2.2 A licensee that provides a crypto-asset based payment service must record and maintain a separate book entry for each customer in relation to any assets belonging to the customer that are received from, or on account of, the customer. Each book entry must contain:

(a) particulars of every transaction carried out on behalf of the customer, including:

i. a description and the quantity of assets that are the subject of the transaction;

ii. the price and fee arising from the transaction;

iii. the name of the customer;

iv. the name of the counterparty to the transaction; and

v. the transaction date and settlement or delivery date;

(b) the amount and description of each asset belonging to the customer deposited in an account held under fiduciary arrangements and the date of such deposit;

(c) the date, quantity and purpose of each transfer of assets belonging to the customer from or to any account held under fiduciary arrangements;

PS-2.2 Additional Requirements for PSPs Offering Crypto-Asset Based Payment Services (continued)

(d) whether the customer has an account held under fiduciary arrangements by the licensee solely for that customer, or shares the same account held under fiduciary arrangements with other customers of the licensee; and
(e) the name of each safeguarding person with whom the licensee deposits any assets belonging to the customer.

PS-2.2.3 A licensee that provides a crypto-asset based payment service must:
(a) ensure that the systems and controls concerning the assessment and management of risks in relation to the safeguarding of assets belonging to a customer are adequate and appropriate for the scale and nature of its operations;
(b) take all reasonable measures to maintain the integrity and security of the means used to safeguard instruments relating to the crypto-assets belonging to a customer;
(c) develop and implement effective controls and segregation of duties to mitigate the risk of conflict between its duties relating to the safeguarding of assets belonging to a customer and its business interests (where such arrangement was allowed by the CBB);
(d) develop and implement written policies and procedures to identify, address and monitor the risk of conflict between its duties relating to the safeguarding of assets belonging to a customer and its business interests; and
(e) ensure that the safeguarding of assets belonging to a customer is not performed by, or performed under the influence or direction of, persons who execute payment transactions.

PS-2.2 Additional Requirements for PSPs Offering Crypto-Asset Based Payment Services (continued)

PS-2.2.4 A licensee that provides a crypto-asset based payment service must, by the end of every business day, complete a computation of:

(a) the total amount of assets belonging to its customers deposited in account held under fiduciary arrangements, as at the end of the previous business day;

(b) the total amount of assets belonging to its customers required under this module to be deposited in account held under fiduciary arrangements as at the end of the previous business day; and

(c) the total amount of the licensee's residual interests in accounts, being assets belonging to the licensee that are deposited in those accounts together with, and commingled with, assets belonging to its customers, as at the end of the previous business day.

Maintain the result of each computation and all data that supports each such computation, for a period of at least 5 years.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-3:	Payment Standards

PS-3.1 Framework Contracts

PS-3.1.1 Before the payment service user utilises a payment service the PSP must make available, in an easily accessible manner, the following information and conditions:

(a) on the payment service provider:

i. the name of the payment service provider, the geographical address of its head office and any other address, including electronic mail address, relevant for communication with the payment service provider; and

ii. the fact the PSP is licensed by the CBB and the license number for identification;

(b) on the initial or first use of the payment service:

i. a description of the payment service to be provided;

ii. a specification of the information or unique identifier that has to be provided by the payment service user in order for a payment order to be properly placed or executed;

iii. the form of and procedure for placing a payment order or giving permission to execute a payment transaction and withdrawal of such permission;

iv. a reference to the time of receipt of a payment order in accordance and the cut-off time, if any, established by the payment service provider;

v. the maximum execution time for the payment services to be provided;

vi. the estimated time for the funds to be received by the payee in his account located outside Bahrain; and

vii. whether there is a possibility to agree on transaction limits for the use of the payment instrument;

(c) on charges, interest and exchange rates:

i. all charges payable by the payment service user to the payment service provider and, where applicable, the breakdown of the amounts of such charges; and

ii. where applicable, the estimated charges for currency conversion services expressed as a percentage mark-up;

PS-3.1 Framework Contracts (continued)

(d) on communication:

i. where applicable, the means of communication, including the technical requirements for the payment service user's equipment and software, agreed between the parties for the transmission of information or notifications under this Module;

ii. the manner in, and frequency with which, information under this Module is to be provided or made available;

iii. the language or languages in which the framework contract will be concluded and communication during that contractual relationship undertaken; and

iv. the payment service user's right to receive the contractual terms of the framework contract and information and conditions;

(e) on safeguards and corrective measures:

i. where applicable, a description of the steps that the payment service user is to take in order to keep safe a payment instrument and how to notify the payment service provider for any loss or theft;

ii. the secure procedure for notification of the payment service user by the payment service provider in the event of suspected or actual fraud or security threats;

iii. where agreed, the conditions under which the payment service provider reserves the right to block a payment instrument;

iv. the liability of the payer in case of unauthorised transactions;

v. how and within what period of time the payment service user is to notify the payment service provider, and the police in case of fraud, of any unauthorised or incorrectly initiated or executed payment transaction or of any authorised transaction made following an incorrect application of the name and unique identifier matching verification service or fraud;

vi. the payment service provider's liability for unauthorised payment transactions, for the incorrect application of the name and unique identifier matching verification service and for fraud;

PS-3.1 Framework Contracts (continued)

vii. the liability of the payment service provider for the non-execution or defective execution of payment transactions; and

viii. the conditions for refund;

(f) on changes to, and termination of, the framework contract:

i. on procedures for changes to framework contracts;

ii. the duration of the framework contract; and

iii. the right of the payment service user to terminate the framework contract;

(g) on redress:

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

ii. where applicable, the alternative dispute resolution procedures available to the payment service user.

PS-3.1.2 Licensees must comply with the following for changes in the framework contract:

(a) Provide any changes in the framework contract or in the information and conditions no later than 2 months before their proposed date of application;

(b) The payment service user can either accept or reject the changes before the date of their proposed date of entry into force;

(c) The changes are deemed to have been accepted if the payment service user does not notify the payment service provider before the proposed date of their entry into force that they are not accepted; and

(d) Exchange rates may be changed without prior notification to the customer, provided such right was agreed in the framework contract and such rates are calculated in a neutral manner.

PS-3.1.3 Framework contracts can be terminated by the customer at any time free of any charges. PSPs may terminate a framework contract concluded for an indefinite period by giving at least 2 months' notice.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-3:	Payment Standards

PS-3.2 Information Requirements

PS-3.2.1 In the case of an individual payment transaction initiated by the payer under a framework contract, a payment service provider must, at the payer's request for this specific payment transaction, provide free of charge explicit information on all of the following:

(a) the maximum execution time;
(b) the charges payable by the payer; and
(c) where applicable, a breakdown of the amounts of any charges.

PS-3.2.2 After the amount of an individual payment transaction is debited from the payer's account or, where the payer does not use a payment account, after receipt of the payment order, the payer's payment service provider must provide the payer, without undue delay and free of charge with all of the following information:

(a) a reference enabling the payer to identify the payment transaction and the payee, including the payee's commercial trade name;
(b) the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency used for the payment order;
(c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges;
(d) where applicable, the exchange rate used in the payment transaction by the payer's payment service provider, and the amount of the payment transaction after that currency conversion; and
(e) the debit value date or the date of receipt of the payment order.

PS-3.2.3 Upon receipt of funds, the payee's payment service provider must provide the payee without undue delay and free of charge with all of the following information:

(a) a reference enabling the payee to identify the payment transaction and the payer, and any information transferred with the payment transaction;
(b) the amount of the payment transaction in the currency in which the payee's payment account is credited;
(c) the amount of any charges for the payment transaction and, where applicable, a breakdown of the amounts of such charges;
(d) where applicable, the exchange rate used in the payment transaction by the payee's payment service provider, and the amount of the payment transaction before that currency conversion; and
(e) the credit value date.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-3:	Payment Standards

PS-3.2 Information Requirements (continued)

PS-3.2.4 **Framework contracts must include a condition that the payer or payee may require the information referred to in Paragraphs 3.2.2 and 3.2.3 to be provided or made available periodically, at least once a month, free of charge and in an agreed manner which allows the payer or payee to store and reproduce information unchanged.**

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-3:	Payment Standards

PS-3.3 Account Information Service Providers and Payment Initiation Service Providers

PS-3.3.1 Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs) must access payment account data exclusively via the dedicated interface provided by account servicing payment service providers. Licensees must at all times:

(a) identify itself towards the account servicing payment service provider;

(b) rely on the authentication procedures provided by the account servicing payment service provider to the payment service user;

(c) take the necessary measures to ensure that they do not process data (including access and storage of data) for purposes other than for the provision of the service as requested by the payment service user; and

(d) log the data that are accessed through the interface operated by the account servicing payment service provider for its payment service users, and provide, upon request the log files to the CBB or relevant authorities. Logs shall be deleted 3 years after their creation. Logs may be kept for longer than this retention period if they are required for monitoring procedures that are already underway.

PS-3.3.2 PISPs must:

(a) provide account servicing payment service providers with the same information as the information requested from the payment service user when initiating the payment transaction directly;

(b) provide services only where based on the payment service user's permission;

(c) not hold at any time the payer's funds in connection with the provision of the payment initiation service;

(d) ensure that the personalised security credentials of the payment services user are not, with the exception of the payer and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;

(e) ensure that any other information about the payment services user obtained when providing payment initiation services, is only provided to the payee and only with the payment services user's permission; and

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-3:	Payment Standards

PS-3.3 Account Information Service Providers and Payment Initiation Service Providers (continued)

(f) every time a payment is initiated, identify itself towards the account servicing payment service provider and communicate with the account servicing payment service provider, the payer and the payee in a secure way.

PS-3.3.3 PISP must not:

(a) store sensitive payment data of the payment service user;
(b) request from the payment service user any data other than those necessary to provide the payment initiation service;
(c) process any personal or non-personal data (including use, access or storage of data) for purposes other than for the provision of the payment initiation service as permitted by the payment services user; and
(d) modify the amount, the payee or any other feature of the transaction.

PS-3.3.4 The AISP must:

(a) provide services only based on the payment service user's permission;
(b) ensure that the personalised security credentials of the payment service user are not accessible to other parties, with the exception of the user and the issuer of the personalised security credentials, and that when those credentials are transmitted by the account information service provider, transmission is done through safe and efficient channels;
(c) for each communication session, identify itself towards the account servicing payment service provider of the payment service user and securely communicate with the account servicing payment service provider and the payment service user;
(d) access only information from designated payment accounts and associated payment transactions; and
(e) have in place suitable and effective mechanisms that prevent access to information other than from designated payment accounts and associated payment transactions, in accordance with the payment service user's permission.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-3:	Payment Standards

PS-3.3 Account Information Service Providers and Payment Initiation Service Providers (continued)

PS-3.3.5 The AISP must not:

(a) request sensitive payment data linked to the payment accounts; and

(b) use, access or store any data for purposes other than for performing the account information service permitted by the payment service user.

PS-3.3.6 A payment transaction or a series of payment transactions must be authorised only if the payer has given its permission for the execution of the payment transaction. A payment transaction may be authorised by the payer prior to or, if agreed between the payer and the account servicing payment service provider, after the execution of the payment transaction.

PS-3.3.7 Access to a payment account for the purpose of account information services or payment initiation services by payment service providers must be authorised only if the payment service user has given its permission to the account information services provider or, respectively, to the payment initiation service provider, to access the payment account and the relevant data in that account. In the absence of permission, a payment transaction or access to a payment account by an AISP or a PISP must be considered to be unauthorised.

PS-3.3.8 The payment service user may withdraw permission to execute a payment transaction or to access a payment account for the purpose of payment initiation services or account information services may be withdrawn by the payment service user at any time. The payment service user may also withdraw permission to execute a series of payment transactions, in which case any future payment transaction must be considered to be unauthorised.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-3:	Payment Standards

PS-3.4 Other Requirements

Issuance and Redeemability of Electronic Money

PS-3.4.1 Issuers of electronic money must issue electronic money at par value of funds received.

PS-3.4.2 Upon request by the holder of the electronic money, the issuer of the electronic money must redeem, at any moment and at par value, the monetary value of the electronic money held.

PS-3.4.3 The framework contract between the issuer of the electronic money and the holder of the electronic money must clearly and prominently state the conditions of redemption, including any applicable fees, and the electronic money holder must be informed of those conditions before being bound by any contract or offer. Any such fee must be proportionate to and commensurate with the actual costs incurred by the electronic money issuer.

PS-3.4.4 Licensees providing electronic money services must not grant to the holder of electronic money interest or any other benefit related to the length of time during which he or she holds the electronic money.

Irrevocability of a Payment Order

PS-3.4.5 The payment service user cannot revoke a payment order once it has been received by the payer's payment service provider, unless:

(a) it is a direct debit, the payer may revoke the payment order at the latest by the end of the business day preceding the day agreed for debiting the funds, subject to receiving the payee's consent; and

(b) it is a future dated payment, the payment service user may revoke a payment order at the latest by the end of the business day preceding the agreed day.

Amounts Transferred and Amounts Received

PS-3.4.6 The payment service provider of the payer, the payment service provider(s) of the payee and any intermediaries of the payment service providers must transfer the full amount of the payment transaction and refrain from deducting charges from the amount transferred.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-4:	Customer Protection Standards

PS-4.1 Customer Protection Standards

PS-4.1.1 This chapter is applicable to PSPs offering account issuance and/or e-money issuance services for retail customer capable of electronic payments.

Contact Information and Notifications

PS-4.1.2 The licensee must request the account holder of a payment account to provide the licensee with contact information in order for the licensee to send the account holder notification alerts for transactions, activation of digital security token and the conduct of high-risk activities. Where the payment account is a joint account, the account holders should jointly give instructions to the licensee on whether the licensee should send transaction notifications to any or all the account holders. High-risk activities include, but are not limited to:

(a) Adding of payees to the account holder's payment profile;
(b) Increasing the transaction limits for outgoing payment transactions from the payment account;
(c) Disabling transaction notifications that the licensee will send upon completion of a payment transaction; and
(d) Change in the account holder's contact information including mobile number, email address and mailing address.

PS-4.1.3 The licensee must at a minimum obtain the following contact information:

(a) Where the account holder has opted to receive notification alerts by SMS, his mobile phone number; or
(b) Where the account holder has opted to receive notification by email, his email address.

Guidance to Account Holders

PS-4.1.4 The licensees required to provide relevant guidance to customers in order to help them protect their accounts. Refer to Appendix PS-1 for guidance on what should be provided to the customers.

Request Information on Unauthorised Transaction

PS-4.1.5 Licensees must request the account holder of a payment account to provide the following information in case of unauthorised transactions:

(a) the account(s) affected, including the account holder's affected accounts with other PSPs if any;
(b) the account holder's identification information;

PS-4.1 Customer Protection Standards (continued)

(c) the type of authentication device, access code and device used to perform the payment transaction;
(d) the name or identity of any account holder for the payment account;
(e) whether a payment account, authentication device, or access code was lost, stolen or misused and if so:
  (i) the date and time of the loss or misuse;
  (ii) the date and time that the loss or misuse, was reported to the licensee; and
  (iii) the date, time and method that the loss or misuse, was reported to the police;
(f) where any access code is applicable to the payment account:
  (i) how the account holder or any account holder recorded the access code; and
  (ii) whether the account holder or any account holder had disclosed the access code to anyone;
(g) any other relevant information about the unauthorised transaction that is known to the account holder, such as:
  (i) a description of the scam incident, including details of the communications with the suspected scammer(s);
  (ii) details of the remote software downloaded (if any) as instructed by the scammer(s);
  (iii) whether the account holder has received any OTPs and/or transaction notifications sent by the licensee, and where applicable/possible a confirmation from telecommunication operators to verify the receipt status only if the account holder is able to obtain it; and
  (iv) suspected compromised applications (if any) in the account holder's device.

Clickable Links or QR Codes

PS-4.1.6 The licensee must not send clickable links or QR codes via email or SMS to an account holder of a retail customer unless:
(a) it is a link or QR code that only contains information for the account holder and does not lead to a (i) website where the account holder provides his access codes or performs any payment transaction or (ii) platform where the account holder is able to download and install apps; and
(b) the account holder is expecting to receive the email or SMS from the licensee.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-4:	Customer Protection Standards

PS-4.1 Customer Protection Standards (continued)

PS-4.1.7 A licensee must ensure its website address listed on CBB's license directory is accurate and up to date. The contact details reflected on the website and other official sources are up to date.

Conduct of High-Risk Activities

PS-4.1.8 A licensee must impose a cooling off period of at least 12 hours where high-risk activities cannot be performed ("cooling off period"), when a digital security token is activated on a device, or when there is a login to an account issued by a PSP on a new device.

PS-4.1.9 A licensee must inform the account holder of a payment account of the risks and implications of performing high-risk activities and obtain additional customer confirmation, at the point before the account holders perform the high-risk activities.

PS-4.1.10 The licensee must provide notification alerts on a real-time basis, that fulfil the following criteria, to the account holder of a payment account, when his digital security token is activated and any high-risk activities are performed:

(a) The notification alert must be sent to the account holder's existing contact details with the licensee. If the account holder has provided more than one account contact to the licensee, the notification must be sent to every contact selected by the account holder to receive such notifications;
(b) The notification alert must be conveyed to the account holder by way of SMS, email or in-app/push notification;
(c) The notification alert must contain details relevant to the digital security token provisioning and activation or high-risk activity, such as information on the payee added, new transaction limits or a change in contact details; and
(d) The notification alert must contain a reminder for the account holder to contact the licensee if the digital security token provisioning and activation or high-risk activity was not performed by the account holder.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-4:	Customer Protection Standards

PS-4.1 Customer Protection Standards (continued)

Transaction Notification Alerts

PS-4.1.11 A licensee must provide transaction notification alerts that fulfil the following criteria to each account holder of a payment account in respect of all outgoing payment transactions made from the account holder's payment account.

(a) The transaction notification alert must be sent to the account holder's contact. If the account holder has provided more than one account contact to the licensee, the transaction notification alert should be sent to every account contact selected by the account holder to receive such notifications;

(b) The transaction notification alert must be sent on a real time basis for each transaction;

(c) The transaction notification alert must be conveyed to the account holder by way of SMS, email or in-app/push notification;

(d) The transaction notification alert must contain the following information, but the licensee may omit and/or partially mask any confidential information provided that the information provided to the account holder still allows the account holder to identify the transaction as being an authorised transaction or unauthorised transaction:

(i) Information that allows the account holder to identify the payment account such as the payment account number;

(ii) Information that allows the account holder to identify the recipient whether by name or by other credentials such as the recipient's account number;

(iii) Information that allows the licensee to later identify the account holder, the payment account, and the recipient account such as each account number or name of the account holder;

(iv) Transaction amount (including currency);

(v) Transaction time and date;

(vi) Transaction type; and

(vii) If the transaction is for goods and services provided by a business, the trading name of the merchant and where possible, the merchant's reference number for the transaction.

PS-4.1.12 While the licensee must make available to account holders the option to receive transaction notification alerts for all outgoing payment transactions (of any amount) made from the account holder's payment account, if the account holder instructs or has instructed the licensee otherwise, the licensee should provide notification alerts for outgoing transactions in accordance with the account holder's instructions.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-4:	Customer Protection Standards

PS-4.1 Customer Protection Standards (continued)

For example, the licensee may provide outgoing transaction notification alerts to the account holder for amounts higher than a particular amount or only for certain types of outgoing transactions, as instructed by the account holder.

PS-4.1.13 A licensee is encouraged to provide transaction notification alerts with similar information as stipulated in Paragraph PS-4.1.11 for payments to the account holder's payment account ("incoming transaction notifications") as a matter of good practice, as incoming transaction notification alerts provide customers with a fuller view of their payments.

Self-Service Kill Switch

PS-4.1.14 A licensee must provide a kill switch for an account holder to promptly block further mobile and online access to his payment account. This includes disallowing mobile and online payment transfers to third parties. The kill switch must be made available in a prominent manner via the mobile application of the licensee, the kiosks of the licensee (where relevant), or the reporting channel provided by the licensee to report unauthorised transactions.

PS-4.1.15 A licensee must educate every account holder of a payment account how to activate this feature.

Recipient Credential Information

PS-4.1.16 Where transactions are made by way of online platforms, any mobile phone application or device arranged for by a licensee for payment transactions, including a payment kiosk, a licensee must provide an onscreen opportunity for any account holder of a payment account to confirm the payment transaction and recipient credentials before the licensee executes payment transaction. The onscreen opportunity must contain the following information:

(a) information that allows the account holder to identify the payment account to be debited;
(b) the intended transaction amount;
(c) credentials of the intended recipient that is sufficient for the account holder to identify the recipient, which at the minimum must be the recipient's phone number, identification number, account number or name as registered for the purpose of receiving such payments; and
(d) a warning to ask the account holder to check the information before executing the payment transaction.

PS-4.1 Customer Protection Standards (continued)

Reporting Channel

PS-4.1.17 The licensee must provide account holders of payment accounts with a reporting channel that is available at all times for the purposes of reporting unauthorised or erroneous transactions and blocking further access via mobile and online channels to his payment account. The reporting channel must have all the following characteristics:

(a) The reporting channel may be a manned phone line, phone number to which text messages can be sent, online portal to which text messages can be sent, a monitored email address, mobile application of the licensee, or the kiosks of the licensee;

(b) Any person who makes a report through the reporting channel must receive a written acknowledgement of his report through SMS, email, or in-app notification; and

(c) The licensee must not charge a fee to any person who makes a report through the reporting channel for the report or any service to facilitate the report.

Real-time Detection

PS-4.1.18 A licensee must have in place capabilities to detect and block suspected unauthorised transactions at all times. A licensee must also have capabilities to inquire into the authenticity of suspected unauthorised transactions before allowing such transactions to be executed. A licensee must review the effectiveness of its detection parameters for suspected unauthorised transactions on an annual basis, or as and when there are material triggers. Licensees must ensure that the detection mechanisms take into account, at a minimum, each of the following risk-based factors:

(a) lists of compromised or stolen authentication elements;

(b) the amount of each payment transaction;

(c) known fraud scenarios in the provision of payment services;

(d) signs of malware infection in any sessions of the authentication procedure; and

(e) in case the access device or the software is provided by the payment service provider, a log of the use of the access device or the software provided to the payment service user and the abnormal use of the access device or the software.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-4:	Customer Protection Standards

PS-4.1 Customer Protection Standards (continued)

Payment Fraud Risks and Trends

PS-4.1.19 Payment service providers must alert their customers via all appropriate means and media when new forms of payment fraud emerge, taking into account the needs of their most vulnerable groups of customers. Licensees must give their customers clear indications on how to identify fraudulent attempts and warn them as to the necessary actions and precautions to be taken to avoid falling victim of fraudulent actions targeting them, and where they can report fraudulent actions and rapidly obtain fraud-related information.

PS-4.1.20 Payment service providers must conduct training programmes on payment fraud risks and trends at regular intervals (not less than twice a year) for their employees and ensure that their employees are adequately trained to carry out their tasks and responsibilities in accordance with the relevant security policies and procedures to mitigate and manage payment fraud risks.

Strong Customer Authentication

PS-4.1.21 Payment service providers must apply strong customer authentication where the payer:
(a) accesses its payment account online;
(b) accesses payment account information;
(c) places a payment order for an electronic payment transaction; and
(d) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.

PS-4.1.22 Strong customer authentication also applies where payments are initiated through a PISP and when the information is requested through an AISP. However:
(a) Account servicing payment service providers shall allow PISPs and the AISPs to rely on the authentication procedures provided by the account servicing payment service provider to the payment service user;
(b) Where payment account information is accessed by an AISP, the account servicing payment service provider shall only apply strong customer authentication for the first access to payment account data by a given AISP, unless the account servicing payment service provider has reasonable grounds to suspect fraud, but not for the subsequent access to that payment account by that AISP; and

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-4:	Customer Protection Standards

PS-4.1 Customer Protection Standards (continued)

(c) Unless the account servicing payment service provider has reasonable grounds to suspect fraud, AISP shall apply their own strong customer authentication when the payment services user accesses the payment account information retrieved by that AISP at least 180 days after strong customer authentication was last applied.

PS-4.1.23 **Strong customer authentication means an authentication which is based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data. The two or more elements do not necessarily need to belong to different categories, as long as their independence is fully preserved.**

PS-4.1.24 **Payment transactions that are not initiated by the payer but by the payee only are not to be subject to strong customer authentication to the extent that those transactions are initiated without any interaction or involvement of the payer.**

PS-4.1.25 Where the payer has given a mandate authorising the payee to place a payment order for a payment transaction or a series of payment transactions through a particular payment instrument and where the mandate is based on an agreement between the payer and the payee for the provision of products or services, the payment transactions initiated thereafter by the payee on the basis of such a mandate may be qualified as payee initiated transactions, provided that those transactions do not need to be preceded by a specific action of the payer to trigger their initiation by the payee.

PS-4.1.26 Where the mandate of the payer to the payee to place payment orders for transactions is provided through a remote channel with the involvement of the payment service provider, the setting up of such a mandate must be subject to strong customer authentication.

PS-4.1.27 For direct debit payment orders, where the mandate given by the payer to the payee to initiate one or several direct debit transactions is provided through a remote channel with the direct involvement of a payment service provider in the setting up of such a mandate, strong customer authentication must be applied.

PS-4.1.28 Payment transactions without the use of electronic platforms or devices, are not to be subject to strong customer authentication, irrespective of whether or not the execution of the transaction is performed electronically.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-4:	Customer Protection Standards

PS-4.1 Customer Protection Standards (continued)

PS-4.1.29 For the remote placement of a payment orders, the payment service providers must apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee. This also includes payment orders through a payer's device using proximity technology for the exchange of information with the payee's infrastructure, the authentication of which requires the use of internet on the payer's device.

Licensee to Assess Claims and Complete Claims Investigation

PS-4.1.30 A licensee must assess any claim made by any account holder in relation to any unauthorised transaction for the purposes of assessing the account holder's liability and licensee's liability for reimbursement. It must have a proper governance structure and investigation process, involving representatives who are independent from business units to carry out the above assessment. The licensee must communicate the claim resolution process and assessment to the account holder in a timely and transparent manner.

PS-4.1.31 The licensee must complete an investigation of any relevant claim within 21 working days. The licensee must, within these periods, give account holders a written or oral report of the investigation outcome and its assessment. The licensee must seek acknowledgement (which need not be an agreement) from that account holder of the investigation report.

PS-4.1.32 Where the account holder does not agree with the licensee's assessment, the account holder and the licensee may proceed to commence other forms of dispute resolution, including reporting to the CBB.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-4:	Customer Protection Standards

PS-4.1 Customer Protection Standards (continued)

Scheduled System Downtime

PS-4.1.33 During a scheduled system downtime, the licensee is to ensure continued delivery of key services and alternatives, where applicable. The licensee must also ensure that scheduled system downtime is not performed during periods where high volume of transactions are expected.

Erroneus Transactions

PS-4.1.34 The payment service provider must rectify any incorrectly executed payment transactions where the payment service user notifies the payment service provider without undue delay after becoming aware of any such transaction and no later than 13 months after the debit date.

Unclaimed Customer Funds

PS-4.1.35 The payment service provider must make all efforts to return any customer funds that remain unclaimed following failed or incomplete transactions. Licensees must proactively contact the customer and ensure that such funds are returned without undue delay. Under no circumstances may a licensee recognize unclaimed customer balances as income.

PS-5.1 Reimbursement Requirement for Unauthorised Transactions

Application

PS-5.1.1 This chapter applies to all PSPs offering payment services, other than changing physical currency and account information services, to retail customers where said customers have access to the service through an electronic/digital channel.

PS-5.1.2 Where a payment service user denies having authorised an executed payment transaction or claims that the payment transaction was not correctly executed, the burden must be on the payment service provider to prove that the payment transaction was authorised, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency of the service provided by the payment service provider.

PS-5.1.3 If the payment transaction is initiated through a PISP, the burden must be on the PISP to prove that within its sphere of competence, the payment transaction was authorised, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

PS-5.1.4 Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider, including the PISP as appropriate, will in itself not be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence. The payment service provider, including, where appropriate, the PISP, must provide supporting evidence to demonstrate the occurrence of fraud or gross negligence on part of the payment service user.

PS-5.1.5 In the case of an unauthorised payment transaction, the payer's payment service provider must refund the payer the amount of the unauthorised payment transaction within 21 working days after noting or being notified of the unauthorised transaction, except where the payer's payment service provider has reasonable grounds for suspecting fraud committed by the payer. The customer has 13 months time limit to notify the payment service provider of an unauthorised payment transaction occurring.

PS-5.1 Reimbursement Requirement for Unauthorised Transactions (continued)

PS-5.1.6 Where the payer's payment service provider had reasonable grounds for suspecting fraud committed by the payer, the payer's payment service provider must, within 21 working days after noting or being notified of the transaction, do either of the following:

(a) refund the payer the amount of the unauthorised payment transaction if the payer's payment service provider has concluded, after further investigation, that no fraud has been committed by the payer;

(b) provide a justification for refusing the refund and indicate the authorities to which the payer may refer the matter in accordance if the payer does not accept the reasons provided.

PS-5.1.7 Where applicable, the payer's payment service provider must restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

PS-5.1.8 Where the unauthorised payment transaction is initiated through a PISP, the account servicing payment service provider must refund within 21 working days the amount of the unauthorised payment transaction and, where applicable, restore the debited payment account to the state in which it would have been had the unauthorised payment transaction not taken place.

PS-5.1.9 If the PISP is liable for the unauthorised payment transaction, the PISP must immediately compensate the account servicing payment service provider at its request for the losses incurred or sums paid as a result of the refund to the payer. The burden must be on the PISP to prove that, within its sphere of competence, the payment transaction was authorised, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.

MODULE	PS:	Payment Service Requirements
CHAPTER	PS-5:	Fraud Reimbursement Requirements

PS-5.1 Reimbursement Requirement for Unauthorised Transactions (continued)

PS-5.1.10 The payment service provider shall compensate the payer for loss in the following cases:

(a) the loss, theft or misappropriation of a payment instrument was not detectable to the payer prior to a payment, except where the payer has acted fraudulently; or

(b) the loss was caused by acts or lack of action of an employee a payment service provider or of an entity to which its activities were outsourced.

PS-5.1.11 The payer shall bear all of the losses relating to any unauthorised payment transactions if those losses were incurred by the payer acting fraudulently or failing to fulfil one or more of the obligations below with intent or gross negligence:

(a) use the payment instrument in accordance with the terms governing the issue and use of the payment instrument; and

(b) notify the payment service provider, or the entity specified by the payment service provider, without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument, and in any case no later than 13 months.

PS-5.1.12 Where the payer's payment service provider fails to fulfil the obligation to require strong customer authentication, the payer will not bear any financial losses unless the payer has acted fraudulently.

PS-5.1.13 The payer will not bear any financial consequences resulting from use of the lost, stolen or misappropriated payment instrument after notification except where the payer has acted fraudulently. If the payment service provider does not provide appropriate means of notifying fraud or erroneous transactions, the payer will not be liable for the financial consequences resulting from use of that payment instrument, except where the payer has acted fraudulently.

Fraud Reporting

PS-5.1.14 Payment service providers must provide, at least on a quarterly basis, statistical data on fraud relating to different means of payment to the CBB.

Appendix PS-1

"account issuance service" means any of the following services:

(a) the service of issuing a payment account to any person in Bahrain;

(b) any service relating to any operation required for operating a payment account, including:

i. any service (other than a domestic money transfer service or a cross-border money transfer service) that enables money to be placed in a payment account; or

ii. any service (other than a domestic money transfer service or a cross-border money transfer service) that enables money to be withdrawn from a payment account.

"payment account" means

(a) means any account, or any device or facility (whether in physical or electronic form), that:

i. is held in the name, or associated with the unique identifier, of any person, and is used by that person for the initiation of a payment order or the execution of a payment transaction, or both; or

ii. is held in the names, or associated with the unique identifiers, of 2 or more persons, and is used by any of those persons for the initiation of a payment order or the execution of a payment transaction, or both; and

(b) includes a bank account, debit card, credit card or charge card.

"cross-border money transfer service" means any of the following services:

(a) any service of accepting money in Bahrain, whether as principal or as agent, for the purpose of transmitting, or arranging for the transmission of, the money to any person outside Bahrain;

(b) any service of receiving any money from outside Bahrain for, or arranging for the receipt of any money from outside Bahrain by, any person in Bahrain, whether as principal or as agent; and

(c) any service of arranging for the transmission of money from any country or territory to another country or territory, whether as principal or agent.

"domestic money transfer service" means the service of accepting money for the purpose of executing, or arranging for the execution of, any of the following payment transactions, each of which is between a payer in Bahrain and a payee in Bahrain (except in the case where both the payer and the payee are financial institutions):

(a) a payment transaction executed from, by way of or through a payment account;

(b) a direct debit (including a one-off direct debit) through a payment account;

(c) a credit transfer (including a standing order) through a payment account; and

(d) accepting any money from any person for transfer to the payment account of a different person.

"e-money issuance service" means the service of issuing e-money to any person for the purpose of allowing a person to make payment transactions.

"e-money" means any electronically stored monetary value that:

(a) is denominated in any currency, or pegged by its issuer to any currency;

(b) has been paid for in advance to enable the making of payment transactions through the use of a payment account;

(c) is accepted by a person other than its issuer; and

(d) represents a claim on its issuer but does not include any deposit accepted in Bahrain, from any person in Bahrain.

"merchant acquisition service" means any service of accepting and processing a payment transaction for a merchant under a contract between the provider of the service and the merchant, which results in a transfer of money to the merchant pursuant to the payment transaction, regardless whether the provider of the service comes into possession of any money in respect of the payment transaction, in a case where:

(a) the merchant carries on business in Bahrain, or is incorporated, formed or registered in Bahrain; or

(b) the contract between the provider of the service and the merchant is entered into in Bahrain.

"money-changing service" means the service of buying or selling foreign currency notes.

"crypto-asset based payment service" means undertaking account issuance service, domestic money transfer service, cross-border money transfer service, merchant acquisition service and money-changing service in crypto-assets; where:

(a) crypto-asset means a cryptographically secured digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology but does not include central bank issued digital currencies. It includes payment tokens and stablecoins. Payment tokens are virtual tokens which can be digitally traded and be used for acquiring goods or services or for investment purposes. Payment tokens give rise to no claims on their issuer and are usually decentralised. Stabelcoin means a crypto-asset that seeks to maintain a stable value by reference to a single fiat currency (single currency backed stable coin) or a basket of fiat currencies (multi-currency backed stablecoin) and by holding the fiat currency or fiat currencies, as the case may be, as reserve asset.

(b) Account issuance in the context of crypto-asset means providing an account which may be any password, code, cipher, cryptogram, private cryptographic key or other instrument that enables a person to control access to one or more crypto-assets and/ or to execute a transaction involving one or more crypto-asset, this service includes provision of safeguarding services for the crypto-assets;

(c) Domestic and cross-border money transfer service means any service of arranging (whether as principal or agent) for the transmission of crypto-assets from one crypto-asset account (whether in Bahrain or elsewhere) to another crypto-asset account (whether in Bahrain or elsewhere);

(d) Merchant acquisition service means any service of accepting, as agent of the merchant, crypto assets from one crypto-asset account (whether in Bahrain or elsewhere), for the purposes of transmitting, or arranging for the transmission of, the crypto-assets to a crypto-asset account belonging to the merchant (whether in Bahrain or elsewhere); and

(e) Money-changing service means the buying or selling of crypto-assets in exchange for any money or any other crypto-asset (whether of the same or a different type), where such service is offered regularly and on a centralised basis.

To clarify individuals or businesses holding crypto-assets on their own and transmitting and receiving between themselves on bi-lateral arrangements are not considered to be offering a regulated payment service.

"account servicing payment service provider" means a PSP or a bank providing and maintaining a payment account for a payer.

"payment initiation service" means a service to place a payment order at the request of the payer or of the payee with respect to a payment account held at another payment service provider.

"account information service" means an online service of collecting, either directly or through a technical service provider, and consolidating information held on one or more payment accounts of a payment service user with one or several account servicing payment service providers.

"limited purpose token" means any non-monetary customer loyalty or reward point, any in-game asset, or any similar digital representation of value (crypto-asset tokens) that:

(a) cannot be returned to its issuer, transferred or sold in exchange for money; and

(b) may only be used:

i. in the case of a non-monetary customer loyalty or reward point, for the payment or part payment of, or in exchange for, goods or services, or both, provided by its issuer or any merchant specified by its issuer; or

ii. in the case of an in-game asset, for the payment of, or in exchange for, virtual objects or virtual services within an online game, or any similar thing within, that is part of, or in relation to, an online game.

"limited purpose e-money" means any of the following types of electronically stored monetary value:

(a) any electronically stored monetary value that is, or is intended to be, used only in Bahrain for the payment or part payment of goods or services (or both) provided by the issuer of the electronically stored monetary value;

(b) any electronically stored monetary value that is, or is intended to be, used only in Bahrain in a case where all of the electronically stored monetary value is issued by a public authority or a public authority has undertaken to be fully liable for the value of all of the electronically stored monetary value issued by the issuer of the electronically stored monetary value, in the event of any default by the issuer in honouring a valid payment made using the electronically stored monetary value;

(c) any electronically stored monetary value, that:

i. is issued as part of a scheme, the dominant purpose of which is to promote the purchase of goods, or the use of services, provided by the issuer of the electronically stored monetary value or any merchant specified by that issuer;

ii. is issued to a user of the electronically stored monetary value upon the purchase of goods, or the use of services, provided by the issuer of the electronically stored monetary value or any merchant specified by that issuer;

iii. is not part of a financial product; and

iv. cannot be withdrawn by the user of the electronically stored monetary value, from any payment account maintained for that user, in exchange for currency.

Appendix PS-2

It is the account holder's responsibility to enable notification alerts on any device used to receive notification alerts from the licensee, to opt to receive notification alerts via SMS, email or in-app/push notification for all outgoing payment transactions (of any amount that is above the transaction notification threshold), activation of digital security token and the conduct of high-risk activities made from the account holder's payment account, and to monitor the notification alerts sent to the account contact. The licensee will assume that the account holder will monitor such notification alerts without further reminders or repeat notifications.

Account holder to protect access codes

An account holder should not do any of the following:

(a) voluntarily disclose any access code to any third party, including the staff of any licensee;
(b) disclose the access code in a recognisable way on any payment account, authentication device, or any container for the payment account; or
(c) keep a record of any access code in a way that allows any third party to easily misuse the access code.

If the account holder keeps a record of any access code, he should make reasonable efforts to secure the record, including:

(a) keeping the record in a secure electronic or physical location accessible or known only to the account holder; and
(b) keeping the record in a place where the record is unlikely to be found by a third party.

Account holder to secure access to payment account

An account holder of a payment account should at the minimum do the following where a device is used to access the payment account:

(a) download the licensee's mobile application(s) only from official sources;
(b) update the device's browser to the latest version available;
(c) patch the device's operating systems with regular security updates provided by the operating system provider;
(d) install and maintain the latest anti-virus software on the device, where applicable;
(e) use strong passwords, such as a mixture of letters, numbers and symbols or strong authentication methods made available by the device provider such as facial recognition or fingerprint authentication methods;
(f) not root or jailbreak the devices used; and
(g) not download and install applications from third-party websites outside official sources ("sideload apps"), in particular unverified applications which request device permissions that are unrelated to their intended functionalities.

An account holder should inform all account holders of the security instructions or advice provided by the licensee to the account holder. An account holder should where possible follow security instructions or advice provided by the licensee to the account holder.

An account holder of a payment account should read the content of the messages containing the access codes and verify that the stated recipient or activity is intended prior to completing transactions or high-risk activities.

Account holder to refer to official sources to obtain website addresses and phone numbers

An account holder of a payment account should refer to official sources, e.g., the CBB's license directory, and the licensee's mobile application or the back of cards, e.g. credit card, debit card or charge card ("official sources") to obtain the website addresses and phone numbers ("contact details") of the licensee.

An account holder should not click on links or scan Quick Response codes ("QR codes") purportedly sent by the licensee unless he is expecting to receive information on products and services via these links or QR codes from the licensee. The contents of these links or QR codes should not directly result in the account holder providing any access code or performing a payment transaction or high-risk activity. Such links are only to provide information such as Terms and Conditions, product description, steps to execute a transaction.

Account holder to understand the risks and implications of performing high-risk activities

An account holder of a payment account should read the risk warning messages sent by the licensee before proceeding to confirm the performance of high-risk activities.

If an account holder does not understand the risks and implications of performing high-risk activities, he should access the licensee's website for more information on these activities or contact the licensee prior to performing these activities. When the account holder proceeds to perform the high-risk activities, he is deemed to have understood the risks and implications as presented by the licensee.

Account holder to report unauthorised activities on his payment account

The account holder of a payment account should report any unauthorised activity to the licensee as soon as practicable, and no later than 30 calendar days after receipt of any notification alert for any unauthorised activity, e.g., transactions, high-risk activities, and the activation of a digital security token, that has not been initiated by the account holder or with the account holder's consent.

Account holder to activate self-service feature ("kill switch") provided by the licensee promptly to block further mobile and online access to the payment account

The account holder of a payment account should activate the kill switch provided by the licensee to block further mobile and online access to the payment account, as soon as practicable, after he is notified of any unauthorised transactions and has reason to believe that the account has been compromised, or if he is unable to contact the licensee.

Account holder to make police report

The account holder of a payment account should make a police report as soon as practicable if the licensee requests such a report to be made to facilitate its claims investigation process, or if the account holder suspects that he is a victim of scam or fraud.

Appendix PS-3

Payment Service	Required Submission	Reporting Period
Account issuance service	• Form 1A • Form 1B • Form 1C	Monthly Half-year period Annual period
Domestic money transfer service	• Form 2A • Form 2B • Form 8	Monthly Half-year period Monthly
Cross-border money transfer service	• Form 3A • Form 3B • Form 8	Monthly Half-year period Monthly
Merchant acquisition service	• Form 4A • Form 4B • Form 8	Monthly Half-year period Monthly
E-money issuance service	• Form 5 • Form 8	Monthly Monthly
Crypto-asset based payment service	• Form 6A • Form 6B	Monthly Half-year period
Money-changing service	• Form 7	Annual
Account information and payment initiation services	• Appendix OB-1: Reporting by AISP/PISP	Monthly

SUBMISSION OF REGULATORY RETURNS

(Name of Licensee)

For the Period (Start Date) to (End Date)

Form 1A – Account issuance service (monthly submission)

1 In relation to e-money account issuance services	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
(a) Placement of money in payment accounts issued by the licensee which store e-money		
(b) Withdrawal of money by customers from payment accounts issued by the licensee which store e-money		

2 In relation to account issuance services that are not e-money account issuance services	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
(a) Withdrawal of money by customers from payment accounts issued by the licensee which do not store e-money		
(b) Placement of money in payment accounts issued by the licensee which do not store e-money		

3 Number of payment accounts issued by the licensee for the purposes of enabling a payment service provider to provide:	Total number of accounts as at the end of the reporting period
(a) domestic money transfer services;	
(b) cross-border money transfer services;	
(c) merchant acquisition services;	
(d) e-money issuance services;	
(e) crypto-asset based payment services;	
(f) money-changing services.	

4 Number of customers	Total number of customers at the end of the reporting period

Form 1B – Account-issuance service (semi-annual submission)

1	Total number of customers as at the end of the reporting period	Total value of payment transactions in relation to e-money account issuance services for the reporting period	Total value of payment transactions in relation to account issuance services that are not e-money account issuance services for the reporting period	Total number of payment transactions in relation to account issuance services for the reporting period
(a) Higher risk customers who are politically exposed persons, or family members or close associates of politically exposed persons				
(b) Higher risk customers that do not fall within the scope of sub-paragraph (a)				

2	Total number of customers as at the end of the reporting period
(a) Persons resident in Bahrain	
(b) Persons resident outside Bahrain	

Form 1C – E-money account issuance service (annual submission)

1	Total number of customers at the end of the reporting period	Total number of payment accounts as at the end of the reporting period	Total value of e-money transferred for the reporting period
(a) Number of customers with at least one personal payment account (other than a bearer payment account) that has not been terminated			
(b) Number of personal payment accounts (other than a bearer payment account) that have been issued and have not been terminated			
(c) Of the customers in (a), number of customers who transferred any e-money to an overseas personal deposit account in the name of the customer, and total value of e-money transferred over the reporting period to any overseas personal deposit account in the name of the customer			

Form 2A – Domestic money transfer service (monthly submission)

Payment transactions accepted, processed or executed, for the month, for the purposes of domestic money transfer services.	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period

Form 2B – Domestic money transfer service (semi-annual submission)

	Money accepted for the purpose of conducting domestic money transfers:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
1	From persons resident in Bahrain who are:		
(a)	Natural persons		
(b)	Other persons (includes any company or association or body of persons, corporate or unincorporated)		
2	From persons resident outside Bahrain who are:		
(a)	Natural persons		
(b)	Other persons (includes any company or association or body of persons, corporate or unincorporated)		

3 In relation to domestic money transfer services provided by the licensee, payment transactions that the licensee executes or arranges the execution of, on behalf of:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
(a) higher risk customers who are politically exposed persons, or family members or close associates of politically exposed persons		
(b) higher risk customers who are customers that do not fall within the scope of sub-paragraph (a)		

Form 3A – Cross-Border Money Transfer service (monthly submission)

1	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
Payment transactions accepted, processed or executed, for the purpose of providing any crossborder money transfer service of accepting money in Bahrain, whether as principal or agent, for the purpose of transmitting, or arranging for the transmission of, the money to any person outside Bahrain ("outward cross-border money transfer services")		

2	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
Payment transactions accepted, processed or executed, for the purpose of providing any crossborder money transfer service of receiving any money from outside Bahrain for, or arranging for the receipt of any money from outside Bahrain by, any person in Bahrain whether as principal or as agent ("inward cross-border money transfer services")		

3	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
Payment transactions accepted, processed or executed, for the purpose of providing any crossborder money transfer service of arranging for the transmission of money from any country or territory to another country or territory, whether as principal or agent ("brokering cross-border money transfer services")		

Form 3B – Cross-Border Money Transfer service (semi-annual submission)

In respect of outward cross-border money transfer services, please provide the total value of payment transactions executed and total number of payment transactions where money was accepted from the following—	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
1 Persons resident in Bahrain		
(a) that are financial institutions		
(b) that are not financial institutions:		
(i) natural persons		
(ii) other persons (includes any company or association or body of persons, corporate or unincorporated)		
2 Persons resident outside Bahrain		
(a) that are financial institutions		
(b) that are not financial institutions:		
(i) natural persons		
(ii) other persons (includes any company or association or body of persons, corporate or unincorporated)		

In respect of inward cross-border money transfer services, please provide the total value of payment transactions executed and total number of payment transactions, where money was accepted from the following:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
3 Persons resident in Bahrain		
(a) that are financial institutions		
(b) that are not financial institutions:		
(i) natural persons		
(ii) other persons (includes any company or association or body of persons, corporate or unincorporated)		
4 Persons resident outside Bahrain		
(a) that are financial institutions		
(b) that are not financial institutions:		
(i) natural persons		
(ii) other persons (includes any company or association or body of persons, corporate or unincorporated)		

5 In respect of brokering cross-border money transfer services, please provide the total value of payment transactions executed and total number of payment transactions, where money was accepted from the following:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
Persons that are:		
(a) financial institutions		
(b) not financial institutions:		
(i) natural persons		
(ii) other persons (includes any company or association or body of persons, corporate or unincorporated)		

6 In respect of outward cross-border money transfer services, please provide the total value of payment transactions executed, total number of payment transactions, and name of entity (if applicable), where money was transmitted by the licensee through:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period	Name of entity
(a) a bank			
(b) other financial institutions outside Bahrain			
(c) other licensees			
(d) others (please specify)			

7 In respect of inward cross-border money transfer services, please provide the total value of payment transactions executed, total number of payment transactions, and name of entity (if applicable), where money was transmitted by the licensee through:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period	Name of entity
(a) a bank			
(b) other financial institutions outside Bahrain			
(c) other licensees			
(d) others (please specify)			

8 In respect of brokering cross-border money transfer services, please provide the total value of payment transactions executed, total number of payment transactions, and name of entity (if applicable), where money was transmitted from a country or territory to another country or territory through:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period	Name of entity
(a) a bank			
(b) financial institutions outside Bahrain that do not fall within the scope of sub-paragraph (a)			
(c) others (please specify)			

9 In respect of outward cross-border money transfer services, please provide the total value of payment transactions executed, and total number of payment transactions, where the licensee accepts money:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
(a) from identifiable sources		
(b) from cash sources		
(c) from sources other than those mentioned in sub-paragraphs (a) and (b) above		

10 Please provide the top 10 countries /jurisdictions that—		Beneficiary country / jurisdiction	Total value of payment transactions for the reporting period
(a) money is transmitted to, in respect of outward cross-border money transfer services	1		
	2		
	…		
	10		
		Beneficiary country / jurisdiction	Total value of payment transactions for the reporting period
(b) money is transmitted from, in respect of inward cross-border money transfer services	1		
	2		
	…		
	10		
(c) money is transmitted from, in respect of brokering cross-border money transfer services			

(d) money is transmitted to, in respect of brokering cross-border money transfer services			

		Beneficiary country / jurisdiction	Total value of payment transactions for the reporting period
	1		
	2		
	…		
	10		

		Beneficiary country / jurisdiction	Total value of payment transactions for the reporting period
	1		
	2		
	…		
	10		

11 In relation to cross-border money transfer services provided by the licensee, payment transactions that the licensee executes or arranges the execution of, on behalf of:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
(a) higher risk customers who are politically exposed persons, or family members or close associates of politically exposed persons		
(b) higher risk customers who are customers that do not fall within the scope of sub-paragraph (a)		

12	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
(a) In respect of outward cross-border money transfer services, money sent to higher risk countries / jurisdictions		
(b) In respect of inward cross-border money transfer services, money received from higher risk countries / jurisdictions		
(c) In respect of brokering cross-border money transfer services, money arranged to be transmitted to, or received from, higher risk countries / jurisdictions		

13 In respect of inward cross-border money transfer services, please provide the total value of payment transactions executed, total number of payment transactions, and method of transmission (if applicable), where the payee receives the money by —	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period	Method of transmission
(a) Deposit into payee's bank account			
(b) Delivery of cash / cash cheque to payee			
(c) Others (please specify)			

14		Name of overseas agent(s)	Country / jurisdictions of overseas agent(s)
(a) Overseas agent(s) used for cross-border money transfers (not regulated for AML / CFT)	1		
	2		
	3		
	…		
For each overseas agent listed in 14(a):		Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
(b) Payment transactions accepted, processed or executed by each overseas agent	1		
	2		
	3		
	…		

Form 4A – Merchant Acquisition service (monthly submission)

1 Merchant acquisition payment transactions Payment transactions accepted and processed for:	Total value of payment transactions for the reporting period	Total number of payment transactions for the reporting period
(a) Merchants that are carrying on business in Bahrain, or that are incorporated, formed, or registered in Bahrain		
(b) Merchants that are not carrying on business in Bahrain, and that are not incorporated, formed, or registered in Bahrain		

Form 4B – Merchant Acquisition service (semi-annual submission)

1 Please state the total number of point-of-sale ("POS") terminals you have provided that are:	Number of POS terminals as at the end of the reporting period

2 Total number of merchants for which payment transactions have been accepted or processed, where:	Total number of merchants
(a) the merchants are carrying on business in Bahrain, or are incorporated, formed, or registered in Bahrain	
(b) The merchants are (i) not carrying on business in Bahrain; and (ii) are not incorporated, formed, or registered in Bahrain	

3 List the top 10 merchants by total number of payment transactions that have been accepted or processed, where the merchants are carrying on business in Bahrain, or are incorporated, formed or registered in Bahrain.		Name of Merchant	CR number or other equivalent identification number
	1.		
	2.		
	…		
	9.		
	10.		

Form 5 – E-money Issuance service (monthly submission)

1 All specified e-money Average, over the month, of the total value of specified e-money issued in one day	Average value of specified e-money issued for the reporting period

2 Total balance of e-money issued as at end of reporting period	Total balance e-money issued

Form 6A – Crypto-asset based payment service (monthly submission)

Total value of transactions and total number of transactions executed where Crypto-asset based payment services were provided for the purpose of —	Total value of transactions for the reporting period	Total number of transactions for the reporting period	Total value of crypto-assets held for safeguarding as at end of reporting period
Account Issuance			
Domestic or cross-border money transfer			
Merchant acquisition			
Money changing			

Form 6B – Crypto-asset based payment service (semi-annual submission)

1 Total value of transactions and total number of transactions on behalf of customers where Crypto-asset based payment services referred to in paragraphs (c) or (d) of the definition of "crypto-asset service" were provided for the purpose of —	Total value of transactions for the reporting period	Total number of transactions for the reporting period
(a) Transmission of crypto-assets from one crypto-asset account to another crypto-asset account, controlled by the same PSP		
(b) Sending of crypto-assets from one crypto-asset account to another crypto-asset account that is:		
(i) controlled by another service provider that is subject to or supervised by a regulatory authority for compliance with AML/CFT requirements;		
(ii) controlled by another service provider that is neither subject to nor supervised by an authority for compliance with AML/CFT requirements;		
(iii) not controlled by any service provider.		
(c) Receipt of digital payment tokens from a crypto-asset payment account that is:		
(i) controlled by another service provider that is subject to or supervised by a regulatory authority for compliance with AML/CFT requirements;		
(ii) controlled by another service provider that is neither subject to nor supervised by an authority for compliance with AML/CFT requirements;		
(iii) not controlled by any service provider.		

2 Types of accounts maintained for the purposes of providing Crypto-asset based payment services as at the end of the reporting period	Total number of accounts at the end of the reporting period	Total number of customers at the end of the reporting period	Total value of transactions executed from, by way of or through these accounts for the reporting period	Total number of transactions executed from, by way of or through these accounts for the reporting period
(a) Accounts issued to persons resident in Bahrain, for the purposes of providing Crypto-asset based payment services, who are –				
(i) Individuals				
(ii) Non-individuals				
(b) Accounts issued to persons resident outside Bahrain, for the purposes of providing Crypto-asset based payment services, who are –				
(i) Individuals				
(ii) Non-individuals				
(c) Accounts that are issued where there is no face-to-face contact with the customer at the point of issuing the account, for the purposes of providing Crypto-asset based payment services				

3 (a) If you maintain Crypto-asset based payment service accounts for the following persons resident in Bahrain, please indicate the total value of such tokens held in all such accounts, as at end of the reporting period:	Total balance as at end of the reporting period
(i) Individuals	
(ii) Non-individuals	
(b) If you maintain Crypto-asset based payment service accounts for the following persons resident outside of Bahrain, please indicate the total value of such tokens held in all such accounts, as at end of the reporting period:	
(i) Individuals	
(ii) Non-individuals	

4 Types of Crypto-assets		Name of Crypto-asset	Total value of transactions for the reporting period	Total number of transactions for the reporting period
(a) List of top 5 crypto-assets transacted by: (i) Value	1			
	…			
	5			
(ii) Number of transactions	1			
	…			
	5			
(b) List of all transacted crypto-assets assessed to be of higher risk of money laundering and terrorist financing	1			
	2			
	…			

Account statistics		Name of Crypto-asset	Total value as at the end of the reporting period	
(c) List of top 5 crypto-assets held in all accounts by total value as at the end of the reporting period	1			
	…			
	5			
(d) Total value of crypto-assets held in all accounts as at the end of the reporting period				
(e) List of all crypto-assets assessed to be of higher risk of money laundering and terrorist financing held in all accounts	1			
	2			
	…			

5 Transactions assessed to be of higher risk for money laundering and terrorist financing	Total value of transactions for the reporting period	Total number of transactions for the reporting period
(a) Transactions where crypto-assets are sent to high-risk countries / jurisdictions		
(b) Transactions where crypto-assets are received from high-risk countries / jurisdictions		

(c) Transactions where crypto-assets are sent to wallet addresses on which anonymity-enhancing technologies are applied		
(d) Transactions where crypto-assets are received from wallet addresses on which anonymity-enhancing technologies are applied		

6 In relation to crypto-assets based payment services provided by the licensee, transactions that the licensee executes or arranges the execution of, on behalf of:	Total number of accounts as at the end of the reporting period	Total value of transactions for the reporting period	Total number of transactions for the reporting period
(a) higher risk customers who are politically exposed persons, or family members or close associates of politically exposed persons			
(b) higher risk customers who are customers that do not fall within the scope of sub-paragraph (a)			

7 Please provide the top 10 countries / jurisdictions, by total value of transactions, other than Bahrain —		Country / jurisdiction	Total value of transactions for the reporting period
(a) to which crypto-assets are sent	1		
	2		
	…		
	10		
(b) from which crypto-assets are received		Country / jurisdiction	Total value of transactions for the reporting period

	1		
	2		
	…		
	10		

8 Correspondent account services	Total number of accounts as at the end of the reporting period	Total value of transactions for the reporting period	Total number of transactions for the reporting period
Where the licensee provides correspondent services accounts or other similar services			

Form 7 – Money-Changing service (annual submission)

	Total value of purchase of foreign currency notes for the reporting period	Total value of sale of foreign currency notes for the reporting period
1. Purchase / sale of foreign currency notes from / to		
(a) Money-changers in Bahrain		
(b) Money-changers outside Bahrain		
(c) Natural persons		
(d) other persons (includes any company or association or body of persons, corporate or unincorporated)		
Total		
Commission, charges, & fees		

	Purchase of foreign currency notes for the reporting period	Sale of foreign currency notes for the reporting period
2. Payment transactions above BD 1,000		
(a) Total value of payment transactions		
(b) Total number of payment transactions		

3. Payment transactions with higher risk customers		Total value of purchase of foreign currency notes for the reporting period	Total value of sale of foreign currency notes for the reporting period
(a) Total value of payment transactions			
(b) Total number of payment transactions			
4. Top 10 currencies traded during the reporting period		Foreign currencies	Total value of purchase of foreign currency notes for the reporting period
(a) Total value of foreign currencies purchased	1		
	…		
	10		
(b) Total value of foreign currencies sold		Foreign currencies	Total value of sale of foreign currency notes for the reporting period
	1		
	…		
	10		

Form 8 – Safeguarding (monthly submission)

1 Client money Daily total amount of client money for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Day	Daily balance
	1	
	2	
	…	
	30	
	31	
2 Client money Daily total amount of client money for the purposes of e-money issuance services	Day	Daily balance
	1	
	2	
	…	
	30	
	31	

3 Where relevant money are safeguarded by a guarantee from a safeguarding institution	(a) Name of safeguarding institution 1	Day	Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 1	
			Total client money received by the licensee for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Total client money received by the licensee for the purposes of e-money issuance services
		1		
		2		
		…		
		30		
		31		
			Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 2	

	(b) Name of safeguarding institution 2	Day	Total client money received by the licensee for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Total client money received by the licensee for the purposes of e-money issuance services
		1		
		2		
		…		
		30		
		31		
	(c) Name of safeguarding institution 3	Day	Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 3	
			Total client money received by the licensee for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Total client money received by the licensee for the purposes of e-money issuance services
		1		
		2		
		…		
		30		
		31		

4 Where relevant money are safeguarded by an insurance cover from a safeguarding institution	(a) Name of safeguarding institution 1	Day	Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 1	
			Total client money received by the licensee for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Total client money received by the licensee for the purposes of e-money issuance services
		1		
		2		
		…		
		30		
		31		
	(b) Name of safeguarding institution 2	Day	Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 2	
			Total client money received by the licensee for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Total client money received by the licensee for the purposes of e-money issuance services
		1		
		2		
		…		
		30		
		31		
	(c) Name of safeguarding institution 3	Day	Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 3	
			Total client money received by the licensee for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Total client money received by the licensee for the purposes of e-money issuance services
		1		
		2		
		…		
		30		
		31		

5. Where relevant money is safeguarded under a fiduciary arrangement with a safeguarding institution	(a) Name of safeguarding institution 1	Day	Amount of daily balance in fiduciary account	Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 1	
				Total client money received by the licensee for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Total client money received by the licensee for the purposes of e-money issuance services
		1			
		2			
		…			
		30			
		31			
	(b) Name of safeguarding institution 2	Day	Amount of daily balance in fiduciary account	Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 2	
				Total client money received by the licensee for the purposes of domestic money transfer services, cross border	Total client money received by the licensee for the purposes of e-
				money transfer services, and merchant acquisition services	money issuance services
		1			
		2			
		…			
		30			
		31			
				Daily amount of Client money received by the licensee and safeguarded by safeguarding institution 3	

	(c) Name of safeguarding institution 3	Day	Amount of daily balance in fiduciary account	Total client money received by the licensee for the purposes of domestic money transfer services, cross border money transfer services, and merchant acquisition services	Total client money received by the licensee for the purposes of e-money issuance services
		1			
		2			
		…			
		30			
		31			

6 Changes in safeguarding arrangements			
(a) Commencement of new safeguarding arrangement	Type of Safeguarding arrangement	Safeguarding institution	Effective date
(b) Discontinuation of existing safeguarding arrangement	Type of Safeguarding arrangement	Safeguarding institution	Effective date