



# **AIFC RULES ON PROVIDING MONEY SERVICES (PMS)**

## **AIFC RULES NO. FR00064 OF 2025**

Approval date: 13 April 2025

Astana, Kazakhstan



## CONTENTS

<b>PART 1. GENERAL .....</b>	<b>5</b>
1.1. Application of these Rules .....	5
1.2. Commencement .....	5
1.3. Definitions etc.....	5
<b>PART 2: RULES APPLICABLE TO MONEY SERVICE PROVIDERS .....</b>	<b>6</b>
2.1. Authorisation .....	6
2.2. Requirements for Money Service Provider authorisation .....	6
2.3. Use of Digital Assets and Digital Ledger Technology in providing Money Services.....	6
2.4. Admission of Digital Assets to use in connection with providing Money Services .....	7
2.4.1. General requirements for admission of Digital Assets to use in connection with providing Money Services.....	7
2.4.2. Admission criteria .....	8
<b>PART 3: TECHNOLOGY GOVERNANCE, CONTROLS AND SECURITY .....</b>	<b>10</b>
3.1. Systems and controls.....	10
3.2. Technology governance and risk management framework.....	10
3.3. Incident reporting.....	10
3.4. Cybersecurity policy .....	11
3.5. Management of operational and security risks .....	12
3.6. Testing of IT systems .....	12
3.7. Independent third-party technology governance and IT audit .....	12
3.8. Submitting IT system testing results and report of independent third-party technology governance and IT audit to the AFSA .....	13
3.9. Strong Customer Authentication .....	13
3.9.1. General requirements for Strong Customer Authentication.....	13
3.9.2. Exclusions from Strong Customer Authentication .....	14
3.9.3. Technical standards for Strong Customer Authentication .....	14
<b>PART 4: REQUIREMENTS APPLICABLE TO MONEY SERVICE PROVIDERS THAT ISSUE ELECTRONIC MONEY .....</b>	<b>16</b>
4.1. Issuance and redeemability .....	16
4.2. Conditions of redemption .....	16
4.3. Fees for redemption.....	16
4.4. Amount of redemption.....	16
4.5. Requests for redemption.....	17
4.6. Redemption rights of persons other than Retail Clients.....	17
4.7. Prohibition of interest.....	17
4.8. Termination of a Client Agreement .....	17



4.9.	Reserve Assets.....	17
4.10.	Policies and procedures.....	17
<b>PART 5: INFORMATION REQUIREMENTS.....</b>		<b>19</b>
5.1.	Information for Payer after receipt of the Payment Order.....	19
5.2.	Information for Payer on individual Payment Transactions .....	19
5.3.	Information for Payee after execution .....	19
5.4.	Information requirements for Money Service Providers providing Account Information Services .....	20
5.5.	Changes in agreement information.....	20
<b>PART 6: COMMUNICATION REQUIREMENTS .....</b>		<b>22</b>
6.1.	Communication of information.....	22
6.2.	Charges for information .....	22
6.3.	Currency and information on conversion .....	22
6.4.	Information on additional charges or reductions.....	22
<b>PART 7: RIGHTS AND OBLIGATIONS IN RELATION TO PROVISION OF MONEY SERVICES .....</b>		<b>24</b>
7.1.	No interest or other return permitted.....	24
7.2.	Data protection (Consent for use of personal data).....	24
7.3.	Charges .....	24
7.4.	Consent and withdrawal of consent .....	25
7.5.	Access to Payment Accounts for Payment Initiation Services .....	25
7.6.	Access to Payment Accounts for Account Information Services .....	26
7.7.	Limits on use of Payment Instruments and access to Payment Accounts.....	27
7.8.	Obligations in relation to Payment Instruments and Personalised Security Credentials (on the Client) .....	27
7.9.	Unauthorised / incorrectly executed Payment Transactions.....	28
7.9.1.	Notification and rectification of unauthorised or incorrectly executed Payment Transactions .....	28
7.9.2.	Money Service Provider's liability for unauthorised Payment Transactions .....	28
7.10.	Refunds .....	28
7.10.1	Payment Transactions where the transaction amount is not known in advance.....	28
7.11.	Execution of Payment Transactions.....	29
7.11.1.	Debiting account only on receipt of Payment Orders.....	29
7.11.2.	Grounds for refusal of Payment Orders .....	29
7.11.3.	Revocation of a Payment Order .....	29
7.11.4.	Amounts transferred and amounts received .....	29
7.11.5.	Payment Transactions made to Payment Account.....	29
7.11.6.	Value Date and availability of Funds.....	30
7.12.	Liability for the use of incorrect Unique Identifiers .....	30
7.13.	Right of recourse.....	30



7.14. Disapplication of requirements for bodies corporate.....	31
<b>PART 8: OBLIGATION TO REPORT.....</b>	<b>32</b>
8.1. General reporting requirements .....	32
<b>PART 9: SAFEGUARDING CLIENT MONEY.....</b>	<b>32</b>
9.1. General requirements for safeguarding Client Money.....	32
9.2. Safeguarding Client Money by Investing .....	33
9.3. Relevant Client Money in Providing Money Services .....	34
<b>PART 10: CAPITAL REQUIREMENTS AND CAPITAL RESOURCES.....</b>	<b>36</b>
10.1. Capital requirements for Money Service Providers .....	36
10.1.1. Capital requirements .....	36
10.1.2. Expenditure Based Capital Minimum.....	36
10.1.3. Annual Audited Expenditure.....	36
10.1.4. Electronic Money Capital Requirement .....	37
10.2. CAPITAL RESOURCES.....	38
10.2.1. Calculation of Capital Resources.....	38
<b>PART 11: ACCESS TO PAYMENT SYSTEMS .....</b>	<b>40</b>



## **PART 1. GENERAL**

### **1.1. Application of these Rules**

These Rules, which may be cited as the AIFC Rules on Providing Money Services (“PMS”), apply to a Money Service Provider carrying on Money Services, in or from the AIFC.

### **1.2. Commencement**

These Rules commence on 13 January 2026, except:

- (a) PMS 2.3. (Use of Digital Assets and Digital Ledger Technology in providing Money Services);
- (b) PMS 2.4. (Admission of Digital Assets to use in connection with providing Money Services); and
- (c) Part 10 (Capital Requirements and Capital Resources),

which commence on 13 October 2025.

### **1.3. Definitions**

Terms used in these Rules have the same meanings as they have, from time to time, in the AIFC Glossary.



## PART 2: RULES APPLICABLE TO MONEY SERVICE PROVIDERS

### Guidance

A Money Service Provider is an Authorised Firm to which provisions of the FSFR, GEN, COB, AML, GLO, FEES, BBR, DAA and Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC are applicable either directly or in respect of its officers and Employees who are Approved Individuals or Designated Individuals:

FSFR (in whole);

AML (in whole);

Chapter 1 (Application) of the COB;

Chapter 3 (Communications with Clients and Financial Promotions) of the COB;

Chapter 4 (Key information and client agreement) of the COB;

Chapter 7 (Conflicts of interest) of the COB;

Chapter 8 (Client Assets) of the COB;

Chapter 15 (Complaints handling and dispute resolution) of the COB;

Chapter 16 (Record Keeping and Internal Audit) of the COB;

Schedule 2 (Key Information and Content of Client Agreement) of the COB;

Schedule 5 (Financial Promotions) of the COB;

Chapter 1 (Licensing of Centre Participants) of the GEN;

Chapter 2 (Controlled and Designated Functions) of the GEN;

Chapter 3 (Control of Authorised Persons) of the GEN;

Chapter 4 (Core Principles) of the GEN;

Chapter 5 (Systems and Controls) of the GEN;

Chapter 6 (Supervision) of the GEN;

Chapter 4 (Rules applicable to Authorised Firms Providing Money Services in relation to Digital Assets and issuance of Fiat Stablecoins and Commodity Stablecoins) of DAA;

Chapter 3 (Prudential Reporting Requirements) of the BBR;

Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC.

### 2.1. Authorisation

A Person wishing to carry out the Regulated Activity of Providing Money Services must be an Authorised Firm licensed by the AFSA.

### 2.2. Requirements for Money Service Provider authorisation

The AFSA may not grant authorisation or variation to provide Money Services unless the applicant satisfies all of the following requirements:

- (a) general authorisation requirements applicable to the applicant under the Framework Regulations and other applicable rules, and
- (b) the applicant must ensure that it maintains at all times Capital Resources in accordance with PMS 10.2 to meet the capital requirements set out in PMS 10.1.

### 2.3. Use of Digital Assets and Digital Ledger Technology in providing Money Services

- (1) A Money Service Provider must not use a Digital Asset in connection with providing Money Services under paragraph 21 of Schedule 1 of GEN, except as provided in subrule (2) and DAA 4.1.-1.



- (2) A Money Services Provider may use a Digital Asset in connection with providing Money Services under paragraph 21 of Schedule 1 of GEN if the Digital Asset is:
- (a) issued by an Authorised Firm or has been approved by the AFSA in accordance with PMS 2.4.1 (1);
  - (b) used only for the purposes of Money Services; and
  - (c) sent, held or received in the name of the Money Services Provider and not in the Client's name.

### **Guidance: Use of Digital Assets and Digital Ledger Technology in providing Money Services**

- (1) Pursuant to PMS 2.3, a Money Service Provider is generally prohibited from using Digital Assets in connection with its Money Services business under paragraph 21 of Schedule 1 to GEN. A Money Service Provider that uses Distributed Ledger Technology, including Digital Assets or other similar technology, solely as a technological platform for its Money Service operations under paragraph 21 of Schedule 1 of GEN serving for the sole purpose of facilitating the technology side of the business and supporting the back-office operations shall not be considered as a Digital Asset Service Provider.
- (2) An Authorised Firm that provides Money Services in relation to Digital Assets and issues Fiat stablecoins is considered as a Digital Asset Service Provider and must comply with PMS and Chapter 4 of DAA (Rules applicable to Rules Applicable to Authorised Firms Providing Money Services in relation to Digital Assets and issuance of Fiat Stablecoins).
- (3) An Authorised Firm that provides Money Services in relation to Digital Assets and issues Fiat stablecoins may use Digital Assets in connection with providing Money Services under paragraph 21 of Schedule 1 of GEN in accordance with DAA 4.1.-1.

## **2.4. Admission of Digital Assets to use in connection with providing Money Services**

### **2.4.1. General requirements for admission of Digital Assets to use in connection with providing Money Services**

- (1) For the purposes of PMS 2.3. (2) (a), a Money Service Provider may use a Digital Asset in connection with providing Money Services if:
  - (a) the Digital Asset has been admitted to use by the Money Service Provider in connection with providing Money Services in accordance with subrule (3); or
  - (b) the Digital Asset has been admitted to trading on the Authorised Firm that carries on the Regulated Activity of Operating a Digital Asset Trading Facility; or
  - (c) the Digital Asset has been approved by written notice issued by the AFSA for trading on the Authorised Firm that carries on the Regulated Activity of Operating a Digital Asset Trading Facility; or
  - (d) the Digital Asset is issued by a Money Service Provider.
- (2) For the purposes of DAA 4.1.-1., Money Service Provider may use a Digital Asset in connection with providing Money Services if such Digital Asset has been approved by the AFSA for use in providing Money Services in accordance with the procedures set out in subrules (3)(a), (4) and PMS 2.4.2. (1), (2), (3) and (4).



- (3) A Money Service Provider must, before admitting any Digital Asset to use in connection with providing Money Services:
  - (a) be satisfied that the applicable requirements, including those in its internal policies, for admission of Digital Asset to use in connection with providing Money Services, have been or will be fully complied with in respect of the Digital Asset; and
  - (b) obtain approval of the AFSA in respect of Fiat and Commodity stablecoins in accordance with subrule (4), except for stablecoins issued by the Digital Asset Service Providers
- (4) For the purposes of subrule (3) (b), a Money Service Provider must make an application to the AFSA and include:
  - (a) a copy of the admission application; and
  - (b) any other information requested by the AFSA.

#### **2.4.2. Admission criteria**

- (1) For the purposes of PMS 2.4.1 (2) and (3), a Digital Asset can be admitted to use by a Money Service Provider on its facility if the Money Service Provider and the AFSA are satisfied that:
  - (a) having considered the matters in subrule (2), the Digital Asset is suitable for use in the AIFC;
  - (b) the Digital Asset is not prohibited for use in the AIFC; and
  - (c) for a Fiat or Commodity stablecoin, all of the requirements in subrules (4) or (5) as applicable are met in respect of that Fiat or Commodity stablecoin, and conditions in paragraphs (a) and (b) are met.
- (2) The matters referred to in subrule (1)(a), which the Money Service Provider and AFSA considers, are:
  - (a) the regulatory status of the relevant Digital Asset in other jurisdictions, including whether it has been assessed or approved for use in another jurisdiction, and the extent to which the laws and regulations of that jurisdiction are equivalent to the requirements of the AFSA;
  - (b) whether there is adequate transparency relating to the Digital Asset and underlying blockchain, including sufficient detail about its purpose, protocols, consensus mechanism, governance arrangements, founders, key persons, miners and significant holders;
  - (c) the size (the market capitalisation), liquidity and volatility of the market for the Digital Asset globally;
  - (d) whether there is a total limit (cap) for the issuance of Digital Asset;
  - (e) the controls and processes to manage volatility of a particular Digital Asset (tokenomics);
  - (f) the adequacy and suitability of the technology used in connection with the Digital Asset;





- (g) whether risks associated with the Digital Asset are adequately mitigated, including risks relating to governance, legal and regulatory issues, cybersecurity, money laundering, Market Abuse and other Financial Crime;
  - (h) whether a Digital Asset is traceable;
  - (i) whether there are any issues relating to the security or usability of a DLT used for the purposes of a Digital Asset; and
  - (j) whether a DLT and smart contract (if any) have been stress tested or subject to independent audit.
- (3) In assessing the matters in subrule (2), the AFSA may consider the cumulative effect of factors which, if taken individually, may be regarded as insufficient to give reasonable cause to doubt that the criteria in subrule (1)(a) is satisfied.
- (4) In the case of a Fiat stablecoin or Commodity stablecoin backed by a reserve, the additional criteria referred to in subrule (1)(c) are that:
  - (a) information is published at least quarterly on the value and composition of the reserves backing the Fiat stablecoin or Commodity stablecoin;
  - (b) the published information referred to in subrule (4)(a) is verified by a suitably qualified third-party professional who is independent of the issuer of the Digital Asset and any persons responsible for the Digital Asset;
  - (c) the published information referred to in subrule (4)(a) demonstrates that the reserves in respect of Fiat stablecoins:
    - (i) are at least equal in value to the notional value of outstanding Digital Assets in circulation (that value being calculated by multiplying the number of Digital Assets in circulation by the purported pegged Fiat Currency value);
    - (ii) are denominated in the reference currency; and
    - (iii) are held in segregated accounts with properly regulated banks or custodians in jurisdictions with regulation that is equivalent to the AFSA's regime and AML regulation that is equivalent to the standards set out in the FATF Recommendations;
  - (d) the Digital Asset is able to maintain a stable price relative to the Fiat Currency or Commodity it references; and
  - (e) a Person is clearly responsible and liable to investors for the Digital Asset.
- (5) If a Money Service Provider decides to admit a Digital Asset to use in connection with providing Money Services, the Money Service Provider is required to notify the AFSA at least 10 (ten) days prior to the date of the admission of the Digital Asset to use in connection with providing Money Services.



## **PART 3: TECHNOLOGY GOVERNANCE, CONTROLS AND SECURITY**

This Part 3 applies to activities of Providing Money Services in relation to Digital Assets and issuing Fiat stablecoins, except for PMS 3.1. (Systems and controls), PMS 3.2. (Technology governance and risk management framework), 3.4. (Cyber-security policy).

### **3.1. Systems and controls**

- (1) A Money Service Provider must ensure that it implements systems and controls necessary to address the risks, including cybersecurity-related risks, to its business. The relevant systems and controls should take into account such factors that include the nature, scale and complexity of the Money Service Provider's business, the diversity of its operations, the volume and size of transactions made using its facilities and the level of risk inherent within its business and activities.
- (2) A Money Service Provider must have adequate systems and controls to enable it to calculate and monitor its capital requirements and its compliance with the requirements in PMS 10.1. The systems and controls must be in writing and must be appropriate for the nature, scale and complexity of the Money Service Provider's business and its risk profile.

### **3.2. Technology governance and risk management framework**

- (1) A Money Service Provider must implement a technology governance and risk management framework, which must be comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in its business model.
- (2) The technology governance and risk management framework must apply to all technologies relevant to a Money Service Provider's business and clearly set out the Money Service Provider's cybersecurity objectives, including the requirements for the competency of its relevant Employees, and there must be in place clearly defined systems and procedures necessary for managing risks.
- (3) A Money Service Provider must ensure that its technology governance and risk management is capable of determining the necessary processes and controls that it must implement in order to adequately assess, mitigate and monitor any risks identified. In particular, Money Service Provider must ensure that its technology governance and risk management framework includes consideration of international standards and industry best practice codes.
- (4) A Money Service Provider must ensure that its technology governance and risk management framework incorporates appropriate governance policies and system development controls, such as a development, maintenance and testing process for technology systems and operations controls, back-up controls, capacity and performance planning and availability testing.

### **3.3. Incident reporting**

- (1) A Money Service Provider must notify the AFSA as soon as practicable if it becomes aware of a Major Operational or Security Incident.
- (2) A notification under subrule (1) must be in the form and manner, and contain the information, as the AFSA may direct.



- (3) If the incident has, or may have, an impact on the financial interests of its Clients, a Money Service Provider must, as soon as practicable, inform its Clients of the nature of the incident and the measures that the Clients may take to mitigate any adverse effects of the incident.

### **Guidance: Incident reporting**

For the purposes of PMS 3.3.(1), a Major Operational or Security Incident may include a singular event or a series of linked events that are unplanned by the Money Service Provider and that have or will probably have a high adverse impact on Money Services.

### **3.4. Cybersecurity policy**

- (1) A Money Service Provider must establish and implement a cybersecurity policy that outlines procedures for the protection of its electronic systems.
- (2) A Money Service Provider must ensure that its cybersecurity policy is reviewed at least annually by the Employee responsible for information technology security and technology governance. The review must be submitted to the Board of Directors.
- (3) The cybersecurity policy must, at a minimum, address the following areas:
  - (a) information security;
  - (b) data governance and classification;
  - (c) access controls;
  - (d) business continuity and disaster recovery planning and resources, including the plan that ensures, in case of an interruption of its systems and procedures, the preservation of essential data and functions and the maintenance of its activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of its activities;
  - (e) capacity and performance planning;
  - (f) systems operations and availability concerns;
  - (g) systems and network security;
  - (h) systems and application development and quality assurance;
  - (i) physical security and environmental controls, including but not limited to procedures for access to premises and systems;
  - (j) customer data privacy;
  - (k) procedures regarding Client authentication and session controls including, but not limited to, the maximum number of incorrect attempts permitted for entering a password, appropriate time-out controls and password validity periods;
  - (l) procedures for authentication checks where there is a change to a Client's account information or contact details;
  - (m) vendor and third-party service provider management;



- (n) incident response, including, but not limited to, root cause analysis and rectification activities to prevent reoccurrence;
  - (o) governance framework and escalation procedures for decision-making and managing risks, including, but not limited to, responses to ransomware and other cyberattacks; and
  - (p) hardware and infrastructure standards, including, but not limited to, network lockdown, desktop security and firewall standards.
- (4) A Money Service Provider must consider the impact of any outsourcing arrangements, as well as the interoperability risks when dealing with systems and software provided by third parties, where applicable.
- (5) A Money Service Provider must ensure all staff receive appropriate training in relation to cybersecurity.

### **3.5. Management of operational and security risks**

A Money Services Provider must at least annually, or more frequently if requested by the AFSA, conduct a comprehensive assessment of the operational and security risks associated with the Money Services it provides. The Money Services Provider must provide the assessment to the AFSA upon request.

### **3.6. Testing of IT systems**

Before commencing live operations or implementing updates to its IT systems, a Money Service Provider must use development and testing methodologies that align with internationally accepted standards to assess the viability and effectiveness of such systems. The testing must be sufficient to provide reasonable assurance that, among other things:

- (a) the systems enable ongoing compliance with all applicable requirements;
- (b) the systems can operate effectively under stressed market conditions;
- (c) the systems have adequate electronic capacity to handle reasonably foreseeable volumes of messaging and orders; and
- (d) any embedded risk management controls, such as automatic error report generation, function as intended.

### **3.7. Independent third-party technology governance and IT audit**

- (1) The AFSA may require a Money Service Provider to undergo an independent qualified third-party technology governance and IT audit, including vulnerability assessments and penetration testing, taking into account factors such as:
  - (a) the nature, scale and complexity of the business;
  - (b) the diversity of its operations;
  - (c) the volume and size of transactions made using its facilities;
  - (d) the level of risk inherent of its activities; or
  - (e) in the event of Major Operational or Security Incident.



- (2) The frequency of such audits should be commensurate with the criticality of and risk posed by the IT information asset, function or process.
- (3) If required by the AFSA under paragraph (1), a Money Service Provider must:
  - (a) appoint a suitably qualified independent third-party auditor to:
    - (i) carry out an annual audit of the Money Service Provider's compliance with IT, cybersecurity and governance requirements that apply to it; and
    - (ii) produce a written report which sets out the methodology and results of that audit, confirms whether the requirements referred to in this rule have been met and lists any recommendations or areas of concern;
  - (b) demonstrate to the AFSA that the appointed auditor has the necessary expertise and that proper due diligence has been conducted to ensure the auditor's qualifications.

### **3.8. Submitting IT system testing results and report of independent third-party technology governance and IT audit to the AFSA**

A Money Service Provider must provide the results of IT systems test under PMS 3.6. and the written report of independent third-party technology governance and IT audit in PMS 3.7. to the AFSA promptly upon its request.

#### **Guidance:**

Credentials which indicate a qualified independent third-party auditor is suitable to conduct audit of technology governance and IT systems may include:

- (1) designation as a Certified Information Systems Auditor (CISA) or Certified Information Security Manager (CISM) by the Information Systems Audit and Control Association (ISACA);
- (2) designation as a Certified Information Systems Security Professional (CISSP) by the International Information System Security Certification Consortium (ISC);
- (3) accreditation by a recognised and reputable body to certify compliance with relevant ISO/IEC 27000 series standards; or
- (4) accreditation by the relevant body to certify compliance with the Kazakhstani standards in the area of information (cyber) security.

### **3.9. Strong Customer Authentication**

#### **3.9.1. General requirements for Strong Customer Authentication**

- (1) Money Service Provider must apply Strong Customer Authentication where a Client:
  - (a) accesses its Payment Account online, whether directly or through an Account Information Services provider, in any of the following cases:
    - (i) the first time the Payment Account is accessed; or
    - (ii) the Payment Account has not been accessed for 180 days or more;



- (b) places a Payment Order for an electronic Payment Transaction;
  - (c) carries out any action through a remote channel that may imply a risk of payment fraud or other abuses.
- (2) Where a Payer initiates an electronic remote Payment Transaction directly or through a Money Service Provider that provides Payment Initiation Services, the Payment Service Provider must apply Strong Customer Authentication that includes elements which dynamically link the transaction to a specific amount and a specific Payee.
- (3) A Money Service Provider must maintain adequate security measures to protect the confidentiality and integrity of Clients' Personalised Security Credentials.
- (4) A Money Service Provider must allow a Money Service Provider that provides Payment Initiation Services and Account Information Services to rely on the authentication procedures provided by the Money Service Provider to a Client in accordance with PMS 3.9.1

### **3.9.2. Exclusions from Strong Customer Authentication**

- (1) Money Service Provider is not required to apply Strong Customer Authentication under PMS 3.9.1. when:
  - (a) the Client accesses its own Payment Account information;
  - (b) the Client makes a payment of a small amount;
  - (c) the Client makes a payment to a specified beneficiary on a list created by the Client, or under a standing order, where Strong Customer Authentication was applied when the list or standing order was created; or
  - (d) a transfer is made between accounts held by the same Client.
- (2) Payment Transactions that are not initiated by the Payer but by the Payee must not be subject to Strong Customer Authentication to the extent that those transactions are initiated without any interaction or involvement of the Payer.

#### **Guidance**

For the purposes of PMS 3.9.2.(1) (b), a “small amount” may refer to a transaction not exceeding a specified value (e.g. \$50) or a series of transactions not exceeding a specified aggregated amount (e.g. \$150) within a defined period.

### **3.9.3. Technical standards for Strong Customer Authentication**

A Money Service Provider must develop and implement technical standards relating to:

- (a) the implementation of the requirements for Strong Customer Authentication referred to in PMS 3.9.1;
- (b) procedures for applying the exclusions in PMS 3.9.2.;



## AIFC RULES ON PROVIDING MONEY SERVICES (PMS)

- (c) common and secure standards of communication for the purpose of identification, authentication, notification, and sharing information with Clients and other service providers; and
- (d) where applicable, procedures, systems and controls that ensure the reliability and continuity of the interface made available by a provider of Payment Account.



## **PART 4: REQUIREMENTS APPLICABLE TO MONEY SERVICE PROVIDERS THAT ISSUE ELECTRONIC MONEY**

### **4.1. Issuance and redeemability**

A Money Service Provider that issues, redeems and sells Electronic Money must:

- (a) upon receipt of Funds, issue Electronic Money without delay at par value; and
- (b) at the request of the Electronic Money holder, redeem at any time and at par value, the monetary value of the Electronic Money held.

### **4.2. Conditions of redemption**

A Money Service Provider that issues, redeems and sells Electronic Money must ensure that:

- (a) the contract between the Money Service Provider and the Electronic Money holder clearly and prominently states the conditions of redemption, including any fees relating to redemption; and
- (b) the Electronic Money holder is informed of those conditions before being bound by any contract.

### **4.3. Fees for redemption**

- (1) Redemption may be subject to a fee only where the fee is stated in the contract by PMS 4.2. (a) and:
  - (a) the redemption is requested before the termination of the client agreement;
  - (b) the client agreement provides for a termination date, and the Electronic Money holder terminates the client agreement before that date; or
  - (c) the redemption is requested more than one year after the date of termination of the client agreement.
- (2) Any fees for redemption must be proportionate and commensurate with the costs actually incurred by the Money Service Provider.

### **4.4. Amount of redemption**

- (1) Where, before the termination of the client agreement, an Electronic Money holder makes a request for redemption, the Electronic Money holder may request redemption of the monetary value of the Electronic Money in whole or in part, and the Money Service Provider that issues Electronic Money must redeem the amount so requested subject to any fee imposed in accordance with PMS 4.3.
- (2) Where an Electronic Money holder makes a request for redemption on or up to one year after the date of termination of the client agreement, the Money Service Provider that issues Electronic Money must redeem:





- (a) the total monetary value of the Electronic Money held; or
- (b) if the Money Service Provider carries out any business activities other than the issuance, redemption, and sale of Electronic Money, and it is not known in advance what proportion of Funds received by it will be used for Electronic Money, all the Funds requested by the Electronic Money holder.

**4.5. Requests for redemption**

A Money Service Provider that issues, redeems, and sells Electronic Money is not required under PMS 4.1.(b) to redeem the monetary value of Electronic Money if the Electronic Money holder makes a request for redemption more than 6 (six) years after the date of termination of the client agreement.

**4.6. Redemption rights of persons other than Retail Clients**

PMS 4.3 and 4.4 do not apply to any Person, other than a Retail Client, who accepts Electronic Money. In such cases, the redemption rights of that Person must be governed by the contract between that Person and the Money Service Provider.

**4.7. Prohibition of interest**

A Money Service Provider that issues, redeems, and sells Electronic Money must not:

- (a) award interest on the holding of Electronic Money; or
- (b) provide any other benefit related to the length of time during which an Electronic Money holder holds Electronic Money.

**4.8. Termination of a Client Agreement**

For the purposes of this Part, a client agreement between a Money Service Provider and an Electronic Money holder terminates when the right to use Electronic Money for the purpose of making Payment Transactions ceases.

**4.9. Reserve Assets**

A Money Service Provider may issue Electronic Money in Fiat Currencies in compliance with Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC.

**4.10. Policies and procedures**

A Money Service Provider that issues, redeems, and sells Electronic Money must establish, maintain, and implement policies and procedures regarding:

- (a) safeguarding of Client Money, including how it will be paid or placed in a Client Money Account, invested, insured or guaranteed in accordance with PMS 9.1.;
- (b) segregation of Client Money;
- (c) Electronic Money issuance and redemption;
- (d) mechanisms to ensure the liquidity of Electronic Money, including management of safeguarded Client Money and the liquidity risks associated with redemptions.



- (e) recovery and wind-down procedures.



**PART 5: INFORMATION REQUIREMENTS**

**5.1. Information for Payer after receipt of the Payment Order**

- (1) A Money Service Provider acting for the Payer must, immediately after receipt of the Payment Order, provide or make available to the Payer the information specified in subrule (2) in relation to the service provided.
- (2) The information referred to in subrule (1) is:
  - (a) a reference enabling the Payer to identify the Payment Transaction and, where appropriate, information relating to the Payee;
  - (b) the amount of the Payment Transaction in the currency used in the Payment Order;
  - (c) the amount of any charges for the Payment Transaction payable by the Payer and, where applicable, a breakdown of the amounts of such charges;
  - (d) where an exchange rate is used in the Payment Transaction and the actual rate used in the Payment Transaction differs from the rate provided in accordance with COB Schedule 2 paragraph 6 (b) ii, the actual rate used or a reference to it, and the amount of the Payment Transaction after that currency conversion;
  - (e) the date on which the Money Service Provider received the Payment Order; and
  - (f) the maximum execution time of individual Payment Transaction;

**5.2. Information for Payer on individual Payment Transactions**

- (1) A Money Service Provider must, under the client agreement, provide to the Payer the information specified in subrule (2) for each Payment Transaction at least once per month, free of charge.
- (2) The information referred to in subrule (1) is:
  - (a) a reference enabling the Payer to identify the Payment Transaction and, where appropriate, information relating to the Payee;
  - (b) the amount of the Payment Transaction in the currency in which the Payment Account of the Payer is debited or the currency used in the Payment Order;
  - (c) the amount of any charges for the Payment Transaction and, where applicable, a breakdown of the amounts of such charges or the interest payable by the Payer;
  - (d) where applicable, the exchange rate used in the Payment Transaction by the Payer's Money 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.
- (3) The client agreement may include a condition that the Payer may require the information specified in (2) to be provided or made available periodically at least once a month, free of charge and in an agreed manner which enables the Payer to store and reproduce the information unchanged.

**5.3. Information for Payee after execution**



- (1) A Money Service Provider acting for the Payee must, immediately after the execution of the Payment Transaction and at least once per month free of charge, provide or make available to the Payee the information specified in subrule (2).
- (2) The information referred to in subrule (1) is:
  - (a) a reference enabling the Payee to identify the Payment Transaction and, where appropriate, the Payer and any data transmitted with the Payment Transaction;
  - (b) the amount of the Payment Transaction in the currency in which the Funds are at the Payee's disposal;
  - (c) the amount of any charges for the Payment Transaction payable by the Payee and, where applicable, a breakdown of the amount of such charges;
  - (d) where applicable, the exchange rate used in the Payment Transaction by the Payee's Money Service Provider and the amount of the Payment Transaction before that currency conversion; and
  - (e) the credit Value Date.

**5.4. Information requirements for Money Service Providers providing Account Information Services**

A Money Service Providers providing Account Information Services must provide to the Client:

- (a) any pre-client agreement information as may be specified by the AFSA relevant to the service;
- (b) all charges payable by the Client for the service, and, where applicable, a breakdown of those charges.

**5.5. Changes in agreement information**

- (1) Subject to subrule (2), a Money Service Provider must provide the Client with notice of any proposed changes to:
  - (a) the existing terms of the client agreement; or
  - (b) the pre-client agreement information specified by the AFSA,no later than 2 (two) months before the date on which the proposed changes take effect.
- (2) A client agreement may permit the Money Service Provider to make changes unilaterally if the Client does not object before the proposed effective date.
- (3) Where subrule (2) applies, the Money Service Provider must inform the Client that:
  - (a) the Client will be deemed to have accepted the changes in the circumstances referred to in that subrule; and
  - (b) the Client may terminate the client agreement without charge at any time before the proposed effective date.
- (4) Changes to the interest or exchange rates may be applied immediately and without notice if:



## AIFC RULES ON PROVIDING MONEY SERVICES (PMS)

- (a) such a right is agreed under the client agreement and any such changes in interest or exchange rates are based on the Reference Interest or Exchange Rates information which has been provided to the Client in accordance with COB 4; or
  - (b) the changes are more favourable to the Client.
- (5) A Money Service Provider must inform the Client of any change to the interest rate as soon as possible, unless otherwise agreed with the Client regarding frequency or method of disclosure.
- (6) Any change in the interest or exchange rate used in Payment Transactions must be applied in a neutral manner and must not discriminate against Clients.



## **PART 6: COMMUNICATION REQUIREMENTS**

### **6.1. Communication of information**

A Money Service Provider must ensure any information required to be provided to a Client under PMS 5 and 6 is made available:

- (a) in an easily accessible manner;
- (b) in a Durable Medium that can be easily stored and retrieved by the Client;
- (c) in clear and comprehensible form and using easily understandable language;
- (d) in English or in the language agreed by the parties; and
- (e) unless otherwise specified in these Rules, in good time before the service is provided.

### **6.2. Charges for information**

- (1) A Money Service Provider must not impose any charge for providing or making available information required under COB 4, PMS 5 and this Part.
- (2) The Money Service Provider and the Client may agree on charges for information that is provided at the request of the Client where such information:
  - (a) is additional to the information required under by PMS 5 and this Part;
  - (b) is provided more frequently than the frequency specified in PMS 5 and this Part; or
  - (c) is transmitted using a means of communication other than that specified in the client agreement.
- (3) Any charge imposed under subrule (2) must reasonably correspond to the actual cost incurred by the Money Service Provider in providing the information.

### **6.3. Currency and information on conversion**

- (1) Payment Transactions must be executed in the currency agreed between the parties.
- (2) Where a currency conversion service is offered before the initiation of a Payment Transaction:
  - (a) at an automatic teller machine or the point of sale; or
  - (b) by the Payee,

the party offering the currency conversion service must disclose to the Payer all charges and the exchange rate to be used for converting the Payment Transaction.

### **6.4. Information on additional charges or reductions**

- (1) The Payee must inform the Payer of any charge requested or reduction offered by the Payee for using a specific Payment Instrument before the initiation of the Payment Transaction.



## AIFC RULES ON PROVIDING MONEY SERVICES (PMS)

- (2) A Money Service Provider or any relevant other party involved in a Payment Transaction must inform the Client of any charge requested by the Money Service Provider or other party for the use of a specific Payment Instrument before the initiation of Payment Transaction.
- (3) A Payer or Client is not obliged to pay a charge of the type referred to in (1) or (2) if the Payer or Client was not informed of the full amount of the charge in accordance with the relevant subrule.



## **PART 7: RIGHTS AND OBLIGATIONS IN RELATION TO PROVISION OF MONEY SERVICES**

### **7.1. No interest or other return permitted**

A Money Service Provider must not pay any interest or any other form of return on amounts in a Payment Account.

### **7.2. Data protection (Consent for use of personal data)**

A Money Service Provider must not access, process, or retain any Personal Data for the purpose of providing Money Services, unless the conditions set out in the AIFC Data Protection Regulations and AIFC Data Protection Rules are met.

### **7.3. Charges**

- (1) A Money Service Provider may charge the Client only for the fulfilling its obligations under this Part:
  - (a) in accordance with PMS 7.11.4. or 7.12. (2) (b);
  - (b) pursuant to mutual agreement between the parties; and
  - (c) where such charges reasonably correspond to the actual costs incurred by the Money Service Provider.
- (2) Where the Money Service Providers of both the Payer and the Payee, or the only Money Service Provider in respect of a Payment Transaction, are within the AIFC, the respective Money Service Providers must ensure that:
  - (a) the Payee pays any charges levied by the Payee's Money Service Provider; and
  - (b) the Payer pays any charges levied by the Payer's Money Service Provider.
- (3) A Money Service Provider may impose a charge or fee for an Electronic Money redemption only where the relevant charge or fee:
  - (a) is agreed in the client agreement; and
  - (b) relates to early termination or late redemption (that is, a redemption occurring more than 1 (one) year after the termination of the client agreement).
- (4) An Authorised Firm, other than a Money Service Provider that issues Electronic Money, must ensure:
  - (a) any charges payable by the Client on termination are:
    - (i) proportionate to the cost and time of terminating the relevant services; and
    - (ii) not imposed if the termination occurs after 6 (six) months after the date of the client agreement; and





- (b) any amounts prepaid by the Client are reimbursed on termination-

#### **7.4. Consent and withdrawal of consent**

- (1) A Payment Transaction is deemed to have been authorised by the Payer for the purposes of this Part only if the Payer has given consent to:
  - (a) the execution of the Payment Transaction; or
  - (b) the execution of a series of Payment Transactions, of which that Payment Transaction forms part.
- (2) Such consent:
  - (a) may be given before or, if agreed between the Payer and its Money Service Provider, after the execution of the Payment Transaction;
  - (b) must be given in the form and in accordance with the procedure agreed between the Payer and its Money Service Provider; and
  - (c) may be given via the Payee or a Money Service Provider providing Payment Initiation Services.
- (3) The Payer may withdraw its consent to a Payment Transaction at any time before the point at which the Payment Order can no longer be revoked in accordance with client agreement between the Money Service Provider and the Client or under PMS 7.11.3.
- (4) The Payer may withdraw consent to the execution of a series of Payment Transactions at any time, with the effect that any future Payment Transactions will not be regarded as authorised for the purposes of PMS 7.4.

#### **7.5. Access to Payment Accounts for Payment Initiation Services**

Where a Money Service Provider providing Payment Initiation Services accesses a Payment Account which is accessible online, it must:

- (a) not hold a Payer's Funds in connection with the provision of the Payment Initiation Service at any time;
- (b) ensure that a Payer's Personalised Security Credentials are:
  - (i) not accessible to other parties, except for the issuer of the credentials; and
  - (ii) transmitted through secure and efficient channels;
- (c) ensure that no other information about a Payer is provided to any Person except the Payee, and information is provided to the Payee only with the Payer's explicit consent;
- (d) each time it initiates a Payment Order, identify itself to the Money Service Provider and communicate with the Money Service Provider, the Payer and the Payee in a secure way in accordance with the technical standards made under PMS 3.9.3;
- (e) not store Sensitive Payment Data of the Client;



- (f) not request any information from the Payer except that which is required to provide the Payment Initiation Service;
- (g) not use, access or store any information for any purpose other than the provision of the Payment Initiation Service explicitly requested by the Payer;
- (h) not change the amount, the Payee or any other feature of a transaction as notified by the Payer.

**7.6. Access to Payment Accounts for Account Information Services**

- (1) This rule applies only to Payment Accounts accessible online.
- (2) Where a Client uses an Account Information Service, the Money Service Provider providing Account Information Services must:
  - (a) communicate securely with the Money Service Provider providing Account Information Services;
  - (b) immediately after receipt of the Payment Order from the Money Service Provider providing Payment Initiation Services, provide or make available to the Money Service Provider all information regarding the initiation of the Payment Transaction and all information accessible to the Money Service Provider that provides or operates a Payment Account;
  - (c) treat a data request from the Money Service Provider providing Account Information Services in the same manner as a data request received directly from the Payer, unless the Money Service Provider providing or operating the Payment Account has objective reasons to treat the request differently;
  - (d) not require the Money Service Provider providing Account Information Services to enter into a contract before complying with paragraphs (a), (b) and (c).
- (3) Money Service Provider providing Account Information Services must:
  - (a) not provide Account Information Services without the Client's explicit consent;
  - (b) ensure that the Client's Personalised Security Credentials are:
    - (i) not accessible to other parties, except the issuer of the credentials; and
    - (ii) transmitted through safe and efficient channels;
  - (c) for each communication session, identify itself to the Money Service Provider that provides or operates the Payment Account, and communicate securely with the Money Service Provider that provides or operates a Payment Account and the Client;
  - (d) not access any information other than information from designated Payment Accounts and associated Payment Transactions;
  - (e) not request Sensitive Payment Data linked to the Payment Accounts accessed;



- (f) not use, access, or store any information for any purpose except for the provision of the Account Information Service explicitly requested by the Client.

**7.7. Limits on use of Payment Instruments and access to Payment Accounts**

- (1) Where a specific Payment Instrument is used to give consent to the execution of a Payment Transaction, the Payer and the Money Service Provider may agree on spending limits for any Payment Transactions executed through that Payment Instrument.
- (2) A client agreement may provide for the Money Service Provider to have the right to stop the use of a Payment Instrument on reasonable grounds relating to:
  - (a) security concerns regarding the Payment Instrument;
  - (b) suspicion of unauthorised or fraudulent use of the Payment Instrument; or
  - (c) in the case of a Payment Instrument with a credit line, a significantly increased risk that the Payer may be unable to fulfil its liability to pay.
- (3) The Money Service Provider must, in the manner agreed between the Payment Service Provider and the Payer and before taking measures to stop the use of the Payment Instrument:
  - (a) inform the Payer that it intends to stop the use of the Payment Instrument; and
  - (b) provide reasons for doing so.
- (4) Where the Money Service Provider is unable to inform the Payer in accordance with subrule (3) before carrying out any measures to stop the use of the Payment Instrument, it must do so immediately thereafter.
- (5) Subrules (3) and (4) do not apply where the provision of the information in accordance with (3) would compromise reasonable security measures or is otherwise unlawful.
- (6) The Money Service Provider must allow the use of the Payment Instrument or replace it with a new Payment Instrument as soon as practicable after the reasons for stopping its use cease to exist.

**7.8. Obligations in relation to Payment Instruments and Personalised Security Credentials (on the Client)**

- (1) A Client to whom a Payment Instrument has been issued must:
  - (a) use the Payment Instrument in accordance with the terms and conditions applicable to its issuance and use; and
  - (b) notify the Money Service Provider in the agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the Payment Instrument.
- (2) Subrule (1) (a) applies only in relation to terms and conditions that are objective, non-discriminatory and proportionate.



- (3) A Client must take all reasonable steps to keep safe Personalised Security Credentials relating to a Payment Instrument or an Account Information Service.

## **7.9. Unauthorised / incorrectly executed Payment Transactions**

### **7.9.1. Notification and rectification of unauthorised or incorrectly executed Payment Transactions**

A Client is entitled to redress under PMS 7.9.2., only if it notifies the Money Service Provider without undue delay, and in any event no later than 6 (six) months from the date of debit, upon becoming aware of any unauthorised or incorrectly executed Payment Transaction.

### **7.9.2. Money Service Provider's liability for unauthorised Payment Transactions**

- (1) Subject to PMS 7.9.1., where an executed Payment Transaction was not authorised in accordance with PMS 7.4., the Money Service Provider must:
  - (a) refund the amount of the unauthorised Payment Transaction to the Payer; and
  - (b) where applicable, restore the debited Payment Account to the state it would have been in had the unauthorised Payment Transaction not taken place.
- (2) The Money Service Provider must provide the refund referred to in subrule 0 as soon as practicable, and in any event no later than the end of the third Business Day following the day on which it becomes aware of the unauthorised transaction.
- (3) Subrule (2) does not apply if the Money Service Provider has reasonable grounds to suspect fraudulent behaviour by the Client and must notify the relevant authority in accordance with AML 13.8.3 (b). of those grounds in writing.
- (4) When crediting a Payment Account under subrule 0, a Money Service Provider must ensure that the credit Value Date is no later than the date on which the amount of the unauthorised Payment Transaction was debited.
- (5) Where an unauthorised Payment Transaction was initiated through a Money Service Provider providing Payment Initiation Service:
  - (a) the Money Service Provider providing or operating the Payment Account must comply with subrule (1); and
  - (b) if the Money Service Provider providing Payment Initiation Services is liable for the unauthorised Payment Transaction, it must, upon the request of the Money Service Provider providing or operating the Payment Account, compensate the latter immediately for the losses incurred or sums paid as a result of complying with subrule (1), including the amount of the unauthorised transaction.

## **7.10. Refunds**

### **7.10.1 Payment Transactions where the transaction amount is not known in advance**

Where a card-based Payment Transaction is initiated by or through the Payee and the amount of the transaction is not known at the time the Payer authorises the transaction:



- (a) the Payer's Money Service Provider may not block Funds on the Payer's Payment Account unless the Payer has authorised the exact of the Funds amount to be blocked; and
- (b) the Payer's Money Service Provider must release the blocked Funds without undue delay upon becoming aware of the amount of the Payment Transaction, and in any event, immediately upon receipt of the Payment Order.

### **7.11. Execution of Payment Transactions**

#### **7.11.1. Debiting account only on receipt of Payment Orders**

A Money Service Provider must not debit the Client's Payment Account before it has received a Payment Order.

#### **7.11.2. Grounds for refusal of Payment Orders**

- (1) A Money Service Provider that refuses to execute or initiate a Payment Order must, except where it is unlawful to do so, notify the Client:
  - (a) in the agreed manner;
  - (b) no later than on the end of the next business day; and
  - (c) if possible, with the reasons for the refusal.
- (2) A Money Service Provider must also, where applicable, notify the Client of the procedure to rectify any factual errors that led to the refusal.
- (3) A Money Service Provider may not refuse to execute an authorised Payment Order except where:
  - (a) in the circumstances specified in the client agreement, or
  - (b) execution would be unlawful.
- (4) Where the execution of a Payment Order is refused, the Payment Order is deemed not to be received by the Money Service Provider.

#### **7.11.3. Revocation of a Payment Order**

A Money Service Provider must allow the Client to revoke a Payment Order once received by the Money Service Provider if it relates to a future transaction to be executed at least 1 (one) Business Day after the Payment Order is received.

#### **7.11.4. Amounts transferred and amounts received**

The Money Service Provider acting for either a Payer or a Payee must ensure that the full amount of the Payment Transaction is transferred and received, with no charges deducted from the amount transferred, unless such charges have been agreed with both the Payer and Payee.

#### **7.11.5. Payment Transactions made to Payment Account**



The Payer's Money Service Provider must ensure that the amount of the Payment Transaction is credited to the Payee's Money Service Provider's account by the end of the Business Day following receipt of the Payment Order. For a cross-border Payment Transactions involving currency conversions outside Kazakhstan, the credit must occur no later than by the end of fourth Business Day following the receipt of the Payment Order.

### 7.11.6. Value Date and availability of Funds

- (1) The credit Value Date for the Payee's Payment Account must be no later than the Business Day on which the amount of the Payment Transaction is credited to the account of the Payee's Money Service Provider.
- (2) Subrule (1) applies where:
  - (a) the transaction does not involve a currency conversion by the Payee's Money Service Provider;
  - (b) the transaction involves a currency conversion by the Payee's Money Service Provider between any other currency and the Kazakhstani tenge; or
  - (c) the transaction involves only one Money Service Provider.
- (3) The Payee's Money Service Provider must ensure that the amount of the Payment Transaction is at the Payee's disposal immediately after that amount has been credited to that Money Service Provider's account.
- (4) The debit Value Date for the Payer's Payment Account must be no earlier than the time at which the amount of the Payment Transaction is debited to the Payer's Payment Account.

### 7.12. Liability for the use of incorrect Unique Identifiers

- (1) Where a Money Service Provider executes a Payment Order in accordance with a Unique Identifier provided by the Client, the Payment Order shall be deemed correctly executed, regardless of any other information provided by the Client.
- (2) Where a Unique Identifier provided by the Client is incorrect, the Money Service Provider shall not be liable for non-execution or defective execution of the Payment Transaction but:
  - (a) must take reasonable steps to recover the Funds involved in the Payment Transaction; and
  - (b) may, if agreed in the client agreement, charge the Client for recovery of such Funds.

### 7.13. Right of recourse

Where the liability of a Money Service Provider ("the first provider") is attributable to another Money Service Provider or an intermediary, including where there is a failure to apply Strong Customer Authentication as required by PMS 3.9., the other Money Service Provider or intermediary must compensate the first provider for any losses incurred or sums paid pursuant to the provisions set out in this PMS.



**7.14. Disapplication of requirements for bodies corporate**

Where the Client is a body corporate, the Client and the Money Service Provider may agree in writing that the following provisions in PMS shall not apply:

- (a) PMS 6.2.(2) and 6.2. (3) (charges for information);
- (b) PMS 7.4. (3) and (4) (withdrawal of consent);
- (c) PMS 7.9.1 (requests for refund).

The parties may agree that a different time period applies for the purposes of PMS 7.9.1. concerning the reporting of unauthorised or incorrectly executed Payment Transactions.



**PART 8: OBLIGATION TO REPORT**

**8.1. General reporting requirements**

A Money Service Provider must prepare and submit prudential returns and other requested information to AFSA in accordance with relevant provisions of BBR 3.1., 3.4., 3.5., 3.6., 3.7.

**PART 9: SAFEGUARDING CLIENT MONEY**

**9.1. General requirements for safeguarding Client Money**

- (1) Where a Money Service Provider continues to hold relevant Client Money in PMS 9.3 at the end of the Business Day following the day on which it was received, it must safeguard such relevant Client Money in one of the following ways:
  - (a) pay or place of relevant Client Money into a relevant Client Money Account, as prescribed under COB 8; or
  - (b) invest the relevant Client Money in secure, liquid assets in accordance with PMS 9.2. and place those assets in accordance with COB 8.3; or
  - (c) ensure that any relevant Client Money is covered by:
    - (i) an insurance policy with:
      - (A) Authorised Firm conducting Insurance Business; or
      - (B) an insurance firm licensed in a jurisdiction other than AIFC, where the law and practice under which the insurance firm is licensed is broadly equivalent to the AFSA's regulatory regime, ensuring that Clients are afforded protection equivalent to that which they would be afforded if the firm were required to comply with the relevant requirements for the licensing of Authorised Firm conducting Insurance Business, and the insurance firm is regulated in respect of conducting insurance business in such jurisdiction by a regulator to a standard satisfactory to the AFSA;
    - (ii) a comparable guarantee given by an Authorised Firm that carries on Insurance Business or an insurance firm licensed under the conditions specified in subrule (1)(c)
    - (iii) a comparable guarantee given by a Bank or a Regulated Financial Institution.
  - (d) safeguard the relevant Client Money in such other manner approved by the AFSA.
- (2) The proceeds of any insurance policy or guarantee in (1)(c) must be paid upon a Distribution Event into a separate account that:
  - (a) is designated in such a way that it is identifiable as an account held solely for the purpose of safeguarding Client Money in accordance with COB 8; and
  - (b) is used exclusively for holding such proceeds.





- (3) No person other than the Money Service Provider may have any interest in or right over:
  - (a) the relevant Client Money and assets placed in an account in accordance with (1)(a) and (b); or
  - (b) the proceeds placed in an account in accordance with (1)(c).
- (4) A Money Service Provider must maintain organisational arrangements sufficient to minimise the risk of the loss or diminution of Client Money or assets held in accordance with (1)(b), through fraud, misuse, negligence or poor administration.
- (5) When safeguarding relevant Client Money in accordance with (1)(b), a Money Service Provider must establish and maintain the following risk management measures:
  - (a) a Money Service Provider must ensure that its risk management framework includes processes and controls necessary to adequately assess, mitigate and monitor any risks identified in connection with investing Client Money;
  - (b) if a Money Service Provider invests part of the reserves of assets, it must provide a detailed investment policy, including an assessment of the potential impact of such policy on the value of the reserves of assets;
  - (c) policies and procedures must be implemented to ensure Client Money is invested in assets in accordance with PMS 9.2. can be promptly accessed and converted into Fiat Currency at all times, in order to process and complete any redemption or Payment Transactions requests from Clients;
  - (d) the invested assets must be composed and managed in such a manner that addresses liquidity risks associated with the permanent redemption rights of the Clients;
  - (e) any losses, including fluctuations in the value of the financial instruments referred to in subrule (1)(b) and PMS 9.2., must be borne by the Money Service Provider;
  - (f) all profits, losses, and any counterparty or operational risks arising from the investment of Client Money must be borne by the Money Service Provider;
  - (g) at least one of the Approved Individuals must have appropriate experience, knowledge in investing and managing investments.
- (6) A Money Service Provider may not safeguard relevant Client Money in accordance with (1)(b) without the prior written consent of the relevant Client.
- (7) A custodian must comply with the provisions of the Framework Regulations and applicable Rules regarding the provision of custody services, including those set out in COB 8, or, if the custodian is not based in the AIFC, with the rules of the jurisdiction in which the custodian is based, provided these rules ensure a level of protection of Client Money equivalent to that required in the Framework Regulations, applicable Rules, including COB 8.

## **9.2. Safeguarding Client Money by Investing**



For the purposes of subrule (1)(b) of PMS 9.1., assets are considered “secure” (“low risk”) and “liquid” if they fall within following categories:

- (a) Liquid Assets as defined under PRU (INV) 4.3.;
- (b) highly liquid financial instruments with minimal market risk, credit risk, and concentration risk, which can be liquidated rapidly with minimal adverse market impact and have a credit rating of AA (or equivalent) or higher from the globally recognised credit rating agencies (Moody's, Standard & Poor's, or Fitch), including:
  - (i) debt securities issued or guaranteed by central governments, central banks, international organisations, multilateral development banks, regional governments or local authorities;
  - (ii) debt securities issued or guaranteed by bodies corporate;
- (c) Government securities of the Republic of Kazakhstan, issued by the Ministry of Finance of the Republic of Kazakhstan and the National Bank of the Republic of Kazakhstan;
- (d) repurchase agreements with a maturity of 7 (seven) days or less, backed by the assets mentioned in paragraphs (b)(i) and (ii) and (c);
- (e) short-term government money market funds which are backed by the assets mentioned in paragraphs (b)(i) and (ii) and (c);
- (f) Units in a Fund for collective investment in Securities which invests solely in the assets mentioned in paragraphs (b) and (c).

### **Guidance on Safeguarding Client Money by Investing**

- (1) For the purposes of PMS 9.2., “liquid assets” are those that are freely transferrable without restrictions in an active market, with diverse group of buyers and sellers. “Secure assets” are those protected by the institutions against the inherent risks of the assets themselves.
- (2) Investing of Client Money under PMS 9.1.(1)(b) must be made by an Authorised Firm licensed to conduct Regulated Activities of Dealing in Investments as Principal or Managing a Collective Investment Scheme.

### **9.3. Relevant Client Money in Providing Money Services**

- (1) For the purposes of COB 9.1. relevant Client Money includes:
  - (a) sums received from, or for the benefit of, a Client for the execution of a Payment Transaction; and
  - (b) sums received from a Money Service Provider for the execution of a Payment Transaction on behalf of a Client.
- (2) Where:
  - (a) only a portion of the sums referred to in paragraph (1)(a) or (b) is to be used for the execution of a Payment Transaction (with the remainder being used for non-Money Services); and
  - (b) the precise portion attributable to the execution of the Payment Transaction is variable or unknown in advance, the relevant Client Money is the amount that may



## **AIFC RULES ON PROVIDING MONEY SERVICES (PMS)**

be reasonably estimated, based on historical data, to represent the portion attributable to the execution of the Payment Transaction.



## PART 10: CAPITAL REQUIREMENTS AND CAPITAL RESOURCES

### 10.1. Capital requirements for Money Service Providers

#### 10.1.1. Capital requirements

- (1) The capital requirement for a Money Service Provider is calculated as the highest of the following:
  - (a) a base capital of 50,000 USD;
  - (b) the Expenditure-Based Capital Minimum as set out in PMS 10.1.2.; or
  - (c) the Electronic Money Capital Requirement as set out in PMS 10.1.4.
- (2) If a Money Service Provider carries on the Regulated Activity of Providing Money Services in addition to one or more other Regulated Activities or types of Money Services, the highest amount of calculated capital requirement applies.

#### Guidance: Capital requirements

- (1) An Authorised Firm that provides Money Services in relation to Digital Assets and issuing Fiat stablecoins must calculate its capital requirements in compliance with DAA 4.2.(b) and DAA 4.11.3 (ongoing capital relevant for issuer of Fiat stablecoins).
- (2) Such Authorised firm must determine its Capital Resources in accordance with PMS 10.2 to meet the capital requirement under DAA 4.2.(b) and DAA 4.11.3 (ongoing capital relevant for issuer of Fiat stablecoins).
- (3) Pursuant to PMS 10.1.1. (2), where an Authorised Firm combines Money Services under paragraph 21 of Schedule 1 of GEN with Providing Money Services in relation to Digital Assets, issuance of Fiat stablecoins, the highest amount of the calculated capital requirement under DAA 4.2.(b), DAA 4.11.3. and PMS 10.1.1. applies.

#### 10.1.2. Expenditure Based Capital Minimum

A Money Service Provider must calculate its Expenditure-Based Capital Minimum as an amount equal to 10 % of its Annual Audited Expenditure, calculated in accordance with PMS 10.1.3.

#### 10.1.3. Annual Audited Expenditure

- (1) Subject to subrule (2), the Annual Audited Expenditure of a Money Service Provider includes all expenses and losses incurred in the ordinary course of business during a twelve-month accounting period (excluding exceptional items), as recorded in its audited profit and loss account, less the following items (if they are included in the Money Service Provider's audited profit and loss account):
  - (a) staff bonuses, except to the extent that they are non-discretionary;



- (b) Employees' and Directors' shares in profit, including share options, except to the extent that they are non-discretionary;
  - (c) other appropriations of profits, except to the extent that they are automatic;
  - (d) shared commissions and fees payable that are directly related to commissions and fees receivable, which are included with total revenue;
  - (e) fees, brokerage and other charges paid to clearing houses, exchanges or intermediate brokers for executing, registering or clearing transactions;
  - (f) any expenses for which pre-payments or advances have already been made to the respective claimant (e.g. pre-paid rent, pre-paid communication charges, etc.) and deducted from Capital Resources as illiquid assets;
  - (g) foreign exchange losses; and
  - (h) contributions to charities.
- (2) For the purposes of subrule (1)(c), a management charge must not be treated as an appropriation of profits.
- (3) For the purposes of (1), a Money Service Provider must calculate its relevant Annual Audited Expenditure with reference to the Money Service Provider's most recent audited financial statements.
- (4) If the Money Service Provider's most recent audited financial statements do not represent a twelve month accounting period, it must calculate its Annual Audited Expenditure on a pro rata basis so as to produce an equivalent annual amount.
- (5) If the Money Service Provider has not completed its first twelve months of business operations, the Annual Audited Expenditure must be calculated based on forecast expenditure as reflected in the budget for its first twelve months of business operations, as submitted with its application for authorisation.
- (6) A Money Services Provider must recalculate its Annual Audited Expenditure and Expenditure-Based Capital Minimum if:
  - (a) there is a material change in its expenditure (either up or down); or
  - (b) its authorised activities are varied.
- (7) Where a recalculation under subrule (6) is undertaken, the Money Service Provider must submit the recalculated figures to the AFSA within 7 (seven) days. The AFSA may, within 30 (thirty) days of receipt, object to the recalculation and require the Money Service Provider to revise its Expenditure Based Capital Minimum.

### 10.1.4. Electronic Money Capital Requirement

- (1) A Money Service Provider that issues Electronic Money must calculate Electronic Money Capital Requirement in the amount of 1.5% of the average daily outstanding Electronic Money issued by it, where the total volume of issued Electronic Money exceeds USD 3,000,000.
- (2) The Electronic Money Capital Requirement referred to in subrule (1) must consist of Capital Resources calculated in accordance with PMS 10.2.



- (3) The average daily outstanding Electronic Money is the average of the total financial liabilities relating to Electronic Money in issue at the end of each calendar day, where the average is calculated over the previous 6 (six) calendar months.
- (4) A Money Service Provider must perform the calculation under subrule (1) on the first calendar day of each calendar month and must apply the resulting sum as its requirement for that month.
- (5) If a Money Service Provider has not completed its first six months of business operations, the calculation under subrules (3) and (4) must be based on the projected outstanding Electronic Money set out in the business plan submitted with its application for authorisation, subject to any adjustments to that plan required by the AFSA.

## **10.2. CAPITAL RESOURCES**

### **10.2.1. Calculation of Capital Resources**

- (1) For the purposes of PMS, Capital Resources must be calculated as the sum of the following capital elements, subject to deductions listed in subrule (2) below:
  - (a) the ordinary equity share capital of the Money Services Provider, to the extent fully paid up;
  - (b) share premium accounts related to the equity share capital referred to in paragraph (a);
  - (c) any retained earnings, and reserves created out of earnings of past periods, and accumulated other comprehensive income, as defined in the International Financial Reporting Standards (IFRS), to the extent shown in the audited financial statements and accounts of the Money Service Provider; and
  - (d) any amount directed by the AFSA under subrule (3).
- (2) A Money Services Provider must deduct the following items from the sum of the capital elements under subrule (1):
  - (a) any interim losses incurred by a Money Services Provider during the current financial year, irrespective of whether or not shown in audited financial statements and accounts;
  - (b) each of the following, to the extent that its value contributes to the sum of the capital elements in subrule (1):
    - a) goodwill and other intangible assets, as defined in the International Financial Reporting Standards (IFRS);
    - b) tangible fixed assets, including equipment and vehicles;
    - c) deferred tax assets that rely on future profitability;
    - d) defined benefit pension fund assets of the Insurance Intermediary;



## AIFC RULES ON PROVIDING MONEY SERVICES (PMS)

- e) investments by the Money Services Provider or by any of its Subsidiaries in own shares;
- f) holdings of equity shares of Affiliates or Related Persons which a reciprocal cross-holdings with the Money Services Provider, which have the effect of artificially inflating the Capital Resources of the Money Services Provider;
- g) any investments in, and loans to, Affiliates or Related Persons; and
- h) holdings of other investments and assets that are not readily realisable into cash; and
- i) any amount to be deducted from Capital Resources as directed by the AFSA.

3) Where the AFSA is satisfied that a capital instrument issued by the Money Services Provider, and in respect of which the Money Services Provider has received the issuance proceeds in full, has characteristics of permanence and loss absorption that are sufficient to ensure that it would be available to absorb unexpected losses of the Money Services Provider, it may direct that some or all of the liabilities created by that instrument may be included in the Capital Resources of the Money Services Provider under (1)(d).

### **Guidance**

In deciding whether to exercise discretion under subrule (3), the AFSA will take into account whether the capital instrument satisfies the Basel Requirements.



**PART 11: ACCESS TO PAYMENT SYSTEMS**

- (1) A Payment System Operator must have in place objective, non-discriminatory, transparent and proportionate rules governing access to a Payment System by Money Service Providers. Payment System Operators must not restrict access to the Payment System more than is necessary to safeguard against specific risks, including where applicable settlement risk, operational risk, credit risk, liquidity risk and business risk, or more than is necessary to protect the financial and operational stability of the Payment System.
  - (2) A Payment System Operator must make publicly available its rules and procedures for admission to participation in that Payment System and the criteria and methodology it uses for risk assessment of applicants for participation.
  - (3) Upon receipt of an application for participation from a Money Service Provider, a Payment System Operator must assess the relevant risks associated with granting access to the system. A Payment System Operator must refuse participation to an applicant Money Service Provider only where the applicant poses risks to the system, as referred to in subrule (1). The Payment System Operator must notify the applicant in writing, indicating whether the request for participation is granted or refused, and must provide full reasons for any refusal.
  - (4) Subrules (1), (2), and (3) do not apply to Payment Systems composed solely of Money Service Providers that provide Payment Services within the same group.
- (1) A Payment System Operators must not have in place any of the following requirements:
- (a) restrictive rules on effective membership in other Payment Systems;
  - (b) rules which discriminate between Money Service Providers in relation to the rights, obligations and entitlements of members;
  - (c) restrictions based on institutional status.
- (5) A participant of a Payment System that allows a Money Service Provider, that is not a participant of the Payment System, to pass transfer orders through that Payment System must, upon request, give the same possibility to other Money Service Providers in an objective, proportionate, transparent and non-discriminatory manner. In the event of a refusal, the participant must provide full reasons for such refusal to any requesting Money Service Provider.