AIFC ANTI-MONEY LAUNDERING, COUNTER – TERRORIST FINANCING AND SANCTIONS RULES
AIFC RULES NO. FR0008 OF 2017

(with amendments as of 15 December 2024, which commence on 1 January 2025)

Approval Date: 10 December 2017

Commencement Date: 01 January 2018

AIFC ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING AND SANCTIONS RULES

CONTENTS

1. INTRODUCTION

1.1. Overview of the AML Rules

(a) The Anti-Money Laundering Rules (the “AML Rules”) are made in recognition of the application of the Law of the Republic of Kazakhstan No 191-IV dated 28 August 2009 on counteracting legalisation (laundering) of proceeds obtained through criminal means and financing of terrorism (the "AML Law"), the Criminal Code of the Republic of Kazakhstan No 226-V dated 3 July 2014 (the "Criminal Code") and international conventions and treaties ratified by the Republic of Kazakhstan.

(b) In these Rules, a reference to ‘money laundering’ also includes a reference to terrorist financing and financing the proliferation of weapons of mass destruction.

1.2. Purpose of the AML Rules

(a) The AML Rules have been designed to provide a single reference point for all persons and entities (collectively called Relevant Persons) who are supervised by the AFSA for anti-money laundering (“AML”), countering the financing of terrorism ("CFT"), and sanctions compliance. This means that they apply to Authorised Firms, Authorised Market Institutions, Designated Non-Financial Businesses and Professions ("DNFBPs"), FinTech Lab Participants and Registered Auditors.

(b) The AML Rules must not be read in isolation. Relevant Persons must also be aware of the provisions of the Kazakhstan criminal law referred to in Chapter 3 and developments in international policy and best practice. This is particularly relevant when considering United Nations Security Council (“UNSC”) resolutions and unilateral sanctions imposed by other jurisdictions which may apply to a Relevant Person depending on the Relevant Person's jurisdiction of origin, its business and/or customer base.

1.3. [Intentionally omitted]

1.4. Financial Action Task Force

(a) The FATF means the Financial Action Task Force, the inter-governmental body that sets standards, develops and promotes policies, to combat money laundering, and includes any successor entity.

(b) The AFSA has had regard to the FATF Recommendations in making these Rules. A Relevant Person is referred to the FATF Recommendations and interpretive notes to assist it in complying with these Rules. However, if a FATF Recommendation or interpretive note conflicts with a Rule, the relevant Rule takes precedence.

(c) A Relevant Person may also wish to refer to the FATF typology reports which provide information on money laundering methods. These can be found on the FATF website at: www.fatf-gafi.org. Some international groupings, official or informal, publish material that may be useful as context and background in informing the approachadopted by Relevant Persons to AML and CFT. These groupings include Transparency International (www.transparency.org.uk) and the Wolfsberg Group (www.wolfsberg- principles.com).

(d) The Republic of Kazakhstan, as a member of the United Nations, is required to comply with sanctions issued and passed by the UNSC. These Rules contain specific obligations requiring Relevant Persons to establish and maintain effective systems and controls to comply with UNSC resolutions and sanctions (see Chapter 12).

(e) The FATF has issued guidance on a number of specific UNSC resolutions and sanctions regarding the countering of the proliferation of weapons of mass destruction. Such

guidance has been issued to assist in implementing the targeted financial sanctions and activity based financial prohibitions. This guidance can be found on the FATF website at: www.fatf-gafi.org.

(f) In relation to unilateral sanctions imposed in specific jurisdictions such as the European Union, the United Kingdom (HM Treasury) and the United States of America (Office of Foreign Assets Control of the Department of the Treasury), a Relevant Person must consider and take efficient measures to ensure compliance where required or appropriate.

1.5. Structure of the AML Rules

(a) Chapter 2 sets out the application of the AML Rules.

(b) Chapter 3 sets out guidance on relevant Kazakhstan criminal law.

(c) Chapter 4 explains the meaning of the Risk-Based Approach ("RBA"), which must be applied when complying with these Rules and Business Risk Assessment (“BURA”).

(d) Chapter 5 explains the concept of Customer Risk Assessments (“CRA”).

(e) Chapter 6 establishes the Rules for Customer Due Diligence ("CDD") and Chapters 7 and 8 set out the different measures that may be appropriate for higher and lower risk customers - Enhanced Due Diligence ("EDD") and Simplified Due Diligence ("SDD").

(f) Chapter 9 sets out when and how a Relevant Person may rely on a third party to undertake all or some of its CDD obligations. Reliance on a third-party CDD reduces the need to duplicate CDD already performed in respect of a customer. Alternatively, a Relevant Person may outsource some or all of its CDD obligations to a service provider.

(g) Chapter 10 sets out certain obligations in relation to correspondent banking and Chapter11 sets out obligations relating to wire transfers.

(h) Chapter 12 sets out a Relevant Person's obligations in relation to UNSC resolutions and sanctions, and government, regulatory and international findings in relation to AML, CFT, and the financing of weapons of mass destruction.

(i) Chapter 13 sets out the obligation for a Relevant Person to appoint a Money Laundering Reporting Officer ("MLRO") and the responsibilities of this role. It also sets out requirements regarding Threshold Transaction Reports (“TTRs”), Suspicious Transaction Reports ("STRs") that are required to be made under the AML Law and explains the concept of "tipping off".

(j) Chapter 14 sets out general obligations, including requirements for AML training, policies, and record keeping.

1.6. Interpretation

Words and expressions specific to these Rules that require defining are set out in the Annex 1. Other words and expressions used in these Rules are set out in the AIFC Glossary.

Reference to the relevant Rule in these AML Rules is made by reference to “AML” added by the relevant number of the Rule.

2. APPLICATION

2.1. Application

(a) The AML Rules apply to:

(i) every Relevant Person in respect of all its AFSA regulated or supervised activities, except an Authorised Firm licenced to operate a Representative Office or a Credit Rating Agency; and

(ii) the persons specified in AML 2.2. as being responsible for a Relevant Person's compliance with these Rules.

(b) For the purposes of these Rules, a Relevant Person means:

(i) an Authorised Firm;

(ii) an Authorised Market Institution;

(iii) a DNFBP;

(iv) a Registered Auditor; or

(v) a FinTech Lab Participant

Guidance

Only a Centre Participant may be one of the Relevant Persons above. A natural person cannot be a Centre Participant.

2.2. Responsibility for compliance with the AML Rules

(a) Responsibility for a Relevant Person's compliance with these Rules lies with every member of its senior management. Senior management must be fully engaged in ensuring compliance with the AML Rules and must take ownership of the RBA set out in Chapter 4.

(b) In carrying out their responsibilities under these Rules every member of a Relevant Person's senior management must exercise due skill, care and diligence.

(c) Nothing in these Rules precludes the AFSA from imposing disciplinary sanctions, taking enforcement action and any other regulatory action deemed necessary against any person including any one or more of the following persons in respect of a contravention of any AML Rule:

(i) a Relevant Person;

(ii) members of a Relevant Person's senior management; or

(iii) an employee of a Relevant Person.

(d) In these Rules “senior management” means:

In relation to a Relevant Person every member of the Relevant Person’s executive management and includes:

(i) for a AIFC entity, every member of the Relevant Person’s Governing Body;

(ii) for a branch, the person or persons who control the day-to-day operations of the Relevant Person in the AIFC and would include, at a minimum, the senior executive officer or equivalent officer, such as the managing director; and

In relation to a customer that is a body corporate, every member of the body corporate's Governing Body and the person or persons who control the day-to-day operations of the body corporate, including its senior executive officer, chief operating officer and chief financial officer.

2.3. AFSA supervision powers in respect of DNFBPs

The AFSA may conduct reviews of DNFBPs to perform its AML and CFT responsibilities, including as part of its RBA to supervision.

The AFSA may conduct inspections of DNFBPs as part of its RBA to supervising DNFBPs for AML and CFT.

Guidance on AML/ CFT and sanctions supervision

The AFSA receives an annual AML Return from a DNFBP (AML 13.7.) which will assist the AFSA in its supervision of DNFBPs.

Additionally, the AFSA may decide to undertake periodic reviews of one or more DNFBPs as part of its RBA to supervision. The AFSA may also provide further guidance on its approach to AML and CFT supervision of DNFBPs.

The AFSA's reviews may cover matters such as reviewing the firm's systems and controls for conducting a money laundering risk assessment, CDD and complying with applicable resolutions and sanctions of UNSC, as well as other global economic and financial sanctions applicable in the AIFC[1].

Reviews may involve interviews with senior management and a review of relevant records.

[1] List of financial sanctions applicable in the AIFC is presented in the Practical Guidance to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework.

3. GUIDANCE ON KAZAKHSTAN CRIMINAL LAW

3.1. Kazakhstan criminal law

Kazakhstan criminal law applies to all Centre Participants and therefore Relevant Persons must be aware of their obligations in respect of the criminal law as well as these Rules. Relevant Kazakhstan criminal law includes the AML Law and the Criminal Code.

4. THE RISK-BASED APPROACH

4.1. Obligations of the Risk-Based Approach

4.1.1. General Duty

A Relevant Person must take appropriate steps to identify and assess the risks of money laundering to which its business is exposed, and must establish and maintain policies, procedures, systems and controls to mitigate and manage the risks identified.

A Relevant Person must take appropriate steps to manage and mitigate risks considering country-wide risks, including those relevant for the Republic of Kazakhstan identified in the published reports and guidance given by the Financial Intelligence Unit of the Republic of Kazakhstan (the "FIU") regarding the FATF mutual evaluations and follow-up reports, and implement enhanced measures where higher risks are identified.

4.1.2. Nature and size of business

In deciding what steps are appropriate under AML 4.1.1., a Relevant Person must consider the size (as measured by the number of its employees, revenue, or market capitalisation, as appropriate) and nature of its business and the complexity of its activities.

4.1.3. Obligation to assess, manage and mitigate business and customer risks

In order to identify and assess the risks of money laundering a Relevant Person must conduct a business risk assessment and must also conduct customer risk assessments in accordance with Chapter 5 and keep these assessments up to date.

The risks of money laundering that may arise in relation to the development of new products and new business practices, including new delivery mechanisms,and the use of new or developing technologies for both new and pre-existing products must beidentified and assessed by a Relevant Person prior to the launch or use of such products, practices and technologies.

A Relevant Person must take appropriate measures to manage and mitigate the risks identified in its risk assessments.

4.2. Business Risk Assessment by Relevant Persons

4.2.1. Risk factors to be considered for business risk assessment

In carrying out a business risk assessment as required under AML 4.1.1. a Relevant Person must take into account risk factors including:

(a) its customers;

(b) the countries or geographic areas in which it operates;

(c) its products or services;

(d) its transactions;

(e) its delivery mechanisms, channels and partners;

(f) the development of new products and new business practices, including new delivery mechanisms, channels and partners; and

(g) the use of new or developing technologies for both new and pre-existing products.

4.2.2. Use of the business risk assessment

A Relevant Person must use the information obtained from its business risk assessment to:

(a) develop and maintain the policies, procedures, systems and controls required by AML 4.1.1.;

(b) ensure that its policies, procedures, systems and controls adequately mitigate the risks identified;

(c) assess the effectiveness of its policies, procedures, systems and controls;

(d) assist in allocation and prioritisation of AML resources; and

(e) assist in the carrying out of customer risk assessments under Chapter 5.

4.3. Internal policies, procedures, systems and controls

4.3.1. Requirements of policies, procedures, systems and controls

The policies, procedures, systems and controls adopted by a Relevant Person under AML 4.1.1. must be:

(a) proportionate to the nature, scale, complexity and money laundering risks of the activities of the Relevant Person's business;

(b) comprised of, at minimum, organisation of the development and maintenance of the policies, procedures, systems and controls required by AML 4.1.1.:

(i) appropriate representation of AML compliance function in the managing and organising internal control system on AML matters;
(ii) risk management programme (BURA, CRA);
(iii) customer identification programme (KYC/CDD;
(iv) transaction monitoring and reviewing;
(v) employees training and awareness programme;
(vi) adequate screening procedures to ensure high standards when hiring employees (Know Your Employee); and
(vii) independent audit function to test the system.

(c) approved by its senior management; and

(d) monitored, reviewed and updated regularly.

4.3.2. Purpose of policies, procedures, systems and controls

Purpose of policies, procedures, systems and controls is efficient detection of money laundering and terrorist financing (ML/TF), sanctions violation, prevention and minimisation of ML/TF and sanctions risks.

The policies, procedures, systems and controls must provide for the identification and scrutiny of including, but not limited to:

(a) complex or unusually large transactions, or an unusual pattern of transactions;

(b) transactions which have no apparent economic or legal purpose;

(c) other activity which the Relevant Person regards as particularly likely by its nature to be

related to money laundering, sanctions evasion or other financial crimes;

(d) actions aimed at evading proper verification and (or) financial monitoring;

(e) transactions with money and (or) other property, for which there is reason to believe that it is aimed at cashing out money obtained by criminal means; and

(f) transaction with money and (or) other property, the participant of which is a person registered (residing) in a geographic area (state or territory) considered to be an area of high risk.

4.3.3. Record of policies, procedures, systems and controls

A Relevant Person must maintain a written record of the policies, procedures, systems and controls established under AML 4.1.1. The requirements regarding record-keeping for the purposes of this Rule are in AML 14.5.

Guidance on RBA

(a) AML 4.1.1. requires a Relevant Person to adopt an approach to AML which is proportionate to the risks inherent in its business. This is illustrated in Figure 1. The AFSA expects the RBA to be a key part of the Relevant Person's AML compliance culture and to cascade down from the senior management to the rest of the organisation. It requires the full commitment and support of senior management, and the active co-operation of all employees. Embedding the RBA within its business allows a Relevant Person to make decisions and allocate AML resources in the most efficient and effectiveway.

(b) No system of checks will detect and prevent all money laundering. The RBA will, however, balance the cost burden placed on Relevant Persons and their customers, against a realistic assessment of the threat of the Relevant Person's business being used in connection with money laundering. It will focus the effort where it is needed and will have most impact.

(c) In implementing the RBA, a Relevant Person is expected to have in place processes to identify and assess money laundering risks. After the risk assessment, the Relevant Person is expected to monitor, manage and mitigate the risks in a way that is proportionate to the Relevant Person's exposure to those money laundering risks. The general principle is that where there are higher risks of money laundering, a Relevant Person is required to take enhanced measures to manage and mitigate those risks, and that, correspondingly, when the risks are lower, simplified measures are permitted.

(d) The RBA discourages a "tick-box" approach to AML. Instead, a Relevant Person is required to assess relevant money laundering risks and adopt a proportionate response to such risks.

(e) RBA identifies, manages and analyses ML/TF and sanctions risks in order to develop and effectively implement appropriate procedures and controls. It is therefore critical that risk ratings accurately reflect existing risks, provide meaningful assessments leading to practical steps to reduce those risks, are reviewed periodically and, where necessary, regularly updated.

(f) The risk-based analysis should include, among other things, relevant inherent and residual risks at the country, industry, entity itself and business relationship levels. As a result of this analysis, a Relevant Person should develop a thorough understanding of the risks inherent in its customer base, products, delivery channels, services and products offered (pre-existing and new services/products), and the jurisdictions in which it and its customers do business or territories where they are registered from. This understanding should be based on operational, transactional and other internal information collected by the organisation, as well as external sources.

(g) When identifying all ML/TF risks, all relevant information must be considered. This typically requires the input of experts from business, risk management, compliance / legal departments, as well as advice from external experts when necessary. Current and new business products and services should be assessed for vulnerability to money laundering and sanctions violations, and appropriate controls should be put in place before launching them in active stage. There is also a growing number of useful ML/TF risk assessment guidelines available to the public that should be taken into account. For example, published by the FATF, FSRB, regulators and FIU and other agencies such as the UNODC, the IMF, the World Bank, Wolfsberg Group, as well as jurisdiction-specific information, advice and guidance.

(h) Risk is dynamic and requires constant management. It should also be noted that the environment in which every organisation operates is subject to constant change. Externally, political changes in a jurisdiction, as well as the introduction or lifting of economic sanctions, can affect a country's risk rating.

(i) Unless a Relevant Person understands the money laundering and sanctions risks to which it is exposed,it cannot take appropriate steps to prevent its business being used for the purposes of money laundering and sanctions violations. Money laundering risks vary from business to business depending onthe nature of the business, the type of customers a business has, and the nature of the products and services sold.

(j) Relevant Persons that do not offer complex products or services and that have limited international exposure may not need an overly complex or sophisticated business risk assessment, but it should be tailored to the specifics of business and scope of the Relevant Person.

(k) Using the RBA, a Relevant Person assesses its own vulnerabilities to money laundering and takes all reasonable steps to eliminate or manage such risks. The results of this assessment will also feed into the Relevant Person's risk assessment of its customers (see Chapter 6).

(l) Risk management is a continuous process, carried out on a dynamic basis. A money laundering risk assessment is not a one-time exercise. The AFSA expects a Relevant Person's risk management processes for managing money laundering risks are kept under regular review and that any changes made to policies, procedures, systems and controls are recorded.

(m) The Relevant Person should develop and implement the risk assessment model based on quantitative and qualitative characteristics. Numerical values allow to determine the risk category (geography, customer type, products, services, channels used) and the customer's overall risk. Each category can be scored differently, depending on the circumstances of each company's business

5. CUSTOMER RISK ASSESSMENT

5.1. Assessing customer money laundering risks

5.1.1. Requirement to conduct a customer risk assessment

A Relevant Person must:

(a) undertake a risk-based assessment of every customer;

(b) assign the customer a risk rating proportionate to the customer's money laundering risks; and

(c) create customer risk profile based on the CRA procedure.

5.1.2. Timing of the customer risk assessment

The customer risk assessment in AML 5.1.1. must be completed while conducting CDD for new customers, and where, for an existing customer, there is a material change in circumstances.

5.1.3. Conduct of the customer risk assessment

When undertaking a risk-based assessment of a customer under AML 5.1.1. a Relevant Person must:

(a) identify the customer, any beneficial owner(s) and any person acting on behalf of a customer;

(b) obtain information on the purpose and intended nature of the business relationship;

(c) consider the type of customer, its ownership and control structure, and its beneficial ownership (if any);

(d) consider the nature of the customer's business relationship with the Relevant Person;

(e) consider the customer's country of origin, residence, nationality, place of incorporation or place of business;

(f) consider the relevant product, service or transaction;

(g) consider the consistency of the amount of transactions with the provided sources of funds and sources of wealth (SOF/SOW);

(h) consider the beneficiary of a life insurance policy, where applicable; and

(i) consider the outputs of the business risk assessment under Chapter 4.

5.1.4. Identification of Politically Exposed Persons

The policies, procedures, systems and controls adopted by the Relevant Person in accordance with AML 5.1.1. must enable it to determine whether a customer or a beneficial owner is a Politically Exposed Person ("PEP").

5.1.5. Identification of control structure

A Relevant Person must understand the nature of the business and control structure of a customer that is a legal person or legal arrangement.

A Relevant Person must not establish a business relationship with a customer which is a legal person if the ownership or control structure of the customer prevents the Relevant Person from identifying all of the customer's beneficial owners.

5.1.6. Prohibition on relationships with Shell Banks

A Relevant Person must not establish or maintain a business relationship with a Shell Bank.

Guidance on Shell Banks

AML 5.1.6. prohibits a Relevant Person from establishing or maintaining a business relationship with a Shell Bank. The presence of a local agent or administrative staff of a bank would not constitute a physical presence in the country in which the customer is incorporated or licensed.

Guidance on customer risk assessments

(a) The findings of the customer risk assessment will assist the Relevant Person in determining the level of CDD that should be applied in respect of each customer and beneficial owner.

(b) In assessing the nature of a customer, a Relevant Person should consider such factors as the legal structure of the customer, the customer's business or occupation, the location of the customer's business and the commercial rationale for the customer's business model, the pattern of usual behaviour of the customer.

(c) In assessing the customer business relationship, a Relevant Person should consider how the customer is introduced to the Relevant Person and how the customer is serviced by the Relevant Person, including for example, whether the Person will be a private banking customer, will open a bank or trading account, or whether the business relationship will be purely advisory.

(d) The risk assessment of a customer, which is illustrated in Figure 2, requires a Relevant Person to allocate an appropriate risk rating to every customer. Risk ratings areto be described as "low", "medium" or "high" , on a sliding numeric scale, for example with 1 to 3 as "low" risk, 4 to 7 as "medium" risk, and 8 to 10 as "high" risk. Numerical data (value) can be different, depending on the specific of the scoring model of the Relevant Person. Depending on the outcomeof a Relevant Person's assessment of its customer's money laundering risk, a Relevant Person should decide what degree of CDD will need to be conducted.

(e) In AML 5.1.5., ownership arrangements which may prevent the Relevant Person from identifying one or more beneficial owners include bearer shares, nominee shareholder arrangements, and other negotiable instruments in which ownership is determined by possession.

Guidance on the term "customer"

(a) The point at which a person becomes a customer will vary from business to business. However, the AFSA considers that it would usually occur at or prior to the business relationship being formalised, for example, by the signing of a customer agreement or the acceptance of terms of business.

(b) A counterparty would generally be a "customer" for the purposes of these Rules and would therefore require a Relevant Person to conduct CDD on such a person. However, this would not include a counterparty in a transaction undertaken on a Regulated Exchange. Nor would it include suppliers of ordinary business services, to the Relevant Person such

as cleaning, catering, stationery, IT or other similar services.

Guidance on high risk customers

(a) In complying with AML 5.1.1., a Relevant Person should consider customerrisk factors which may indicate that a customer poses a higher risk of money laundering, including, but not limited to:

(i) the business relationship is conducted in unusual circumstances;

(ii) the customer is resident in a geographical area considered by the FATF to be an area of high risk;

(iii) the customer is a legal person or arrangement that is a vehicle for holding personal assets;

(iv) the customer is a company that has nominee shareholders or shares in bearer form;

(v) the customer is a cash-intensive business;

(vi) the corporate structure of the customer is unusual or excessively complex given the nature of the company's business; and

(vii) the customer has been subject to adverse press or public information related to potential money laundering activities.

(b) In complying with AML 5.1.1. a Relevant Person should also consider the following product, service, transaction or delivery channel risk factors:

(i) the product involves private banking;

(ii) the product or transaction is one which might favour anonymity;

(iii) the situation involves non-face-to-face business relationships and/or transactions, without certain safeguards, such as electronic signatures;

(iv) payments will be received from third parties who are unknown to the Relevant Person;

(v) new products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies for new and existing products;

(vi) the service provides nominee directors, nominee shareholders or shadow directors for hire, or offers the formation of companies in third countries;

(vii) the service involves undocumented or verbal agreements with counterparties or customers; and

(viii) the product has unusual complexity or structure and has no obvious economic purpose.

(c) In complying with AML 5.1.1., a Relevant Person should also consider the following geographical risk factors:

(i) countries identified by credible sources, such as FATF mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective systems to counter money laundering; and

(ii) countries subject to sanctions, embargos or similar measures issued by, for example, the UNSC or identified by credible sources as having significant levels of corruption or other criminal activity and countries or geographic areas identified by credible sources as providing funding or support forterrorism.

Guidance on low risk customers

(a) In complying with AML 5.1.1. the following types of customers may pose a lower risk of money laundering:

(i) a governmental entity, or a publicly-owned enterprise from geographical area of lower risk which has AML/CFT regulation, lower level of criminal activities and corruption and which is not identified by credible sources as providing funding or support for terrorism or extremism;

(ii) an individual resident in a geographical area of lower risk which has AML/CFT regulations which are equivalent to the standards set out in the FATF Recommendations;

(iii) Customers with a long-term and active business relationship with the Relevant Person;

(iv) a regulated Financial Institution whose entire operations are subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations; or

(v) a company whose Securities are listed on a Regulated Market in a jurisdiction which has AML regulations which are equivalent to the standards set out in the FATF Recommendations;

(b) In complying with AML 5.1.1. the following types of product, service, transaction or delivery channel risk factors may pose a lower risk of money laundering:

(i) a contract of insurance which is non-life insurance;

(ii) a contract of insurance which is a life insurance product which does not provide for an early surrender option, and cannot be used as collateral;

(iii) a contract of insurance which is life insurance for which the annual premium is low by comparison with prevailing market standards;

(iv) a contract of insurance for the purposes of a pension scheme where the contract contains no surrender clause and cannot be used as collateral;

(v) a pension, superannuation or similar scheme which provides retirement benefits to employees, where contributions are made by an employer or by way of deduction from an employee's wages and the scheme rules do not permit the assignment of a member's interest under the scheme; or

(vi) arbitration, litigation, or advice on litigation prospects.

(c) The assignment of a low risk customer AML rating should not be automatic and should be applied only after an assessment of a customer's actual AML risk as required in AML 5.1.1. In conducting this assessment, however, Relevant Persons should make use of,and build upon, the business risk assessment(s) it has undertaken in accordance with Chapter 4.

6. CUSTOMER DUE DILIGENCE

6.1. Conducting Customer Due Diligence

6.1.1. Obligation to conduct Customer Due Diligence

A Relevant Person must:

(a) conduct CDD under AML 6.3.1. for each of its customers;

(a-a) conduct CDD under AML 6.3.1. for each of its customers including when the customer is carrying out occasional transactions with Digital Assets the value of which singularly or in several linked operations (whether at the time or later), is equal or exceeds USD 1,000;

(a-b) conduct CDD when the customer is carrying out occasional transactions the value of which singularly or in several linked operations (whether at the time or later), is equal or exceeds USD 15,000; and

(b) in addition to (a), (a-a) and (a-b), conduct EDD under AML 7.1.1. in respect of:

(i) each customer it has assigned as high risk;

(ii) business relationships and transactions with persons from a geographic area (state or territory) considered to be an area of high risk.

6.1.2. Conducting Simplified Due Diligence

(a) A Relevant Person may conduct SDD in accordance with AML 8.1.1. by modifying the CDD under AML 6.3.1. for any customer it has assigned as low risk. A Relevant Person must not conduct SDD measures in specific high-risk scenarios or when there is a suspicion of money laundering;

(b) A Relevant Person must ensure that assignment of low risk is based on an adequate risk analysis and SDD is commensurate with the risk level identified.

6.2. Timing of Customer Due Diligence

6.2.1. Establishment of business relationship

A Relevant Person must conduct CDD measures:

(a) when it is establishing a business relationship with a customer; and

(b) after establishing a business relationship with a customer.

6.2.2. After the establishment of a business relationship

A Relevant Person must also conduct appropriate CDD if, at any time:

(a) in relation to an existing customer, it doubts the veracity or adequacy of documents, data or information obtained for the purposes of CDD;

(b) it suspects money laundering; or

(c) there is a change in the risk rating applied by the Relevant Person to an existing customer, or it is otherwise warranted by a change in circumstances of the customer.

6.2.3. Establishing a business relationship before Customer Due Diligence is complete

A Relevant Person may establish or retain a business relationship with a customer before completing the verification required by AML 6.3.1. if the following conditions are met:

(a) deferral of the verification of the customer or beneficial owner is necessary in order not to interrupt the normal conduct of a business relations in the case of securities transactions. In the securities industry, companies and intermediaries may be required to complete transactions very quickly in accordance with market conditions at the time a customer contacts them, and may be required to complete a transaction before identity verification is completed;

(b) risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification have been adopted and are in place; and there is little risk of money laundering occurring and any such risks identified can be effectively managed by the Relevant Person;

(c) in relation to a bank account opening, there are adequate safeguards in place to ensure that the account is not closed and transactions are not carried out by or on behalf of the account holder (including any payment from the account to the account holder) before verification has been completed; and

(d) subject to (c), the relevant verification is completed as soon as reasonably practicable before or during the establishment of a business relationship and when transactions for occasional customers are being conducted; and in any event, no later than 30 days after the establishment of a business relationship.

6.2.4. Inability to complete Customer Due Diligence within 30 days

Where a Relevant Person is not reasonably able to comply with the 30-day requirement in AML6.2.3(d), it must, prior to the end of the 30-day period:

(a) document the reason for its non-compliance;

(b) complete the verification in AML 6.2.3 as soon as possible; and

(c) record the non-compliance event.

6.2.5. Cessation of business

The AFSA may specify a period within which a Relevant Person must complete the verification required by AML 6.2.3. failing which the AFSA may direct the Relevant Person to cease any business relationship with the customer.

Guidance on timing of Customer Due Diligence

(a) For the purposes of AML 6.2.2.(a), examples of situations which might lead a Relevant Person to have doubts about the veracity or adequacy of documents, data or information previously obtained could be where there is a suspicion of money laundering in relation to that customer, where there is a material change in the way that the customer's account is operated, which is not consistent with the customer's business profile, or where it appears to the Relevant Person that a person other than the customer is the real customer or in other cases as referred in AML Law and AIFC acts.

(b) The cases stipulated by AML 6.2.3. are exceptional and do not apply to the most Relevant Persons. Situations that the Relevant Person may take into account include, for example, accepting subscription monies during a short offer period; executing a time critical transaction, which if not executed immediately, would or may cause a customerto incur a financial loss due to price movement or loss of opportunity; and when a customer seeks immediate insurance cover.

(c) When complying with AML 6.2.1., a Relevant Person should also, where appropriate,

consider AML 6.6.1. regarding failure to conduct or complete CDD and Chapter 13 regarding STRs and tipping off.

(d) [intentionally omitted].

(e) Relevant Person needs to adopt risk management procedures with respect to the conditions under which a customer may utilise the business relationship prior to verification, envisaged by AML 6.2.3. These procedures should include a set of measures, such as a limitation of the number, types and/or amount of transactions that can be performed and the limiting or close monitoring of large or complex transactions being carried out outside the expected norms for that type of relationship

6.3. Conducting Customer Due Diligence

6.3.1. Obligation to verify and understand

In conducting CDD required by AML 6.1.1., a Relevant Person must:

(a) verify the identity of the customer and any person acting on behalf of the customer, including his authorisation to so act, based on original or properly certified documents, data or information issued by or obtained from a reliable and independent source;

(a-a) verify the identity of any beneficial owner(s) of the customer;

(b) obtain information on and understand the purpose and intended nature of the business relationship;

(c) understand the customer's SOF according to the CRA;

(d) understand the customer's SOW according to the CRA; and

(e) conduct on-going due diligence of the customer business relationship under AML 6.4.1.

6.3.2. Customer obligation for life insurance

In complying with AML 6.3.1. for life insurance or other similar policies, a Relevant Person must:

(a) verify the identity of customers as soon as reasonably practicable before or during the establishment of a business relationship and when transactions for occasional customers are being conducted;

(b) verify the identity of any named beneficiaries of the insurance policy at the time of pay-out;

(c) verify the identity of the persons in any class of beneficiary, or where these are not identifiable, ensure that it obtains sufficient information to be able to verify the identity of such persons at the time of pay-out;

(d) if a beneficiary of the insurance policy who is a legal person or a legal arrangement presents a higher risk, take enhanced measures which should include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of pay-out;

(e) take reasonable measures to determine whether the beneficiaries of the insurance policy and/or, where required, the beneficial owner of the beneficiary, are PEPs, at the latest, at the time of the pay-out, and, in cases of higher risks, inform senior management before the pay-out of the policy proceeds, conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a STR; and

(f) include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

6.3.3. Customer is a Politically Exposed Person

Where a customer, or a beneficial owner of the customer, is a PEP, a Relevant Person must ensure that, in addition to AML 6.3.1. it also:

(a) increases the level of risk, the degree and nature of monitoring of the business relationship, in order to determine whether the customer's transactions or activities appear unusual or suspicious;and

(b) obtains the approval of senior management to commence a business relationship with the customer.

6.3.4 Existing customer becoming a Politically Exposed Person

A Relevant Person must not continue its business relationship with an existing customer if the customer (or a beneficial owner of the customer) becomes a PEP, unless the Relevant Person obtains the approval of its senior management.

Guidance on conducting Customer Due Diligence

(a) A Relevant Person should, in complying with AML 6.3.1.(a), and adopting the RBA, obtain, verify and record, for every customer who is a natural person, the following identification information:

(i) full name (including any alias);

(ii) date of birth;

(iii) nationality;

(iv) legal domicile; and

(v) current residential address (not a P.O. box).

(b) Items (i) to (iii) above should be obtained from a current valid passport or, where a customer does not possess a passport, an official identification document which includes a photograph. The concept of domicile generally refers to the place which a person regards as his permanent home and with which he has the closest ties or which is his place of origin.

(c) A Relevant Person should, in complying with AML 6.3.1.(a), and adopting the RBA, obtain, verify and record, for every customer which is a legal person, the following identification information:

(i) full business name and any trading name;

(ii) registered or business address;

(iii) date of incorporation or registration;

(iv) place of incorporation or registration;

(v) a copy of the certificate of incorporation or registration;

(vi) a valid commercial or professional licence;

(vii) the identity of the directors, partners, trustees or equivalent persons with executive authority of the legal person or the relevant natural person who is a member of senior management; and

(viii) for a trust, a certified copy of the trust deed to ascertain the nature and purpose of the trust and documentary evidence of the appointment of the current trustees.

(d) In complying with AML 6.3.1.(a), it may not always be possible to obtain original documents. Where identification documents cannot be obtained in original form, for example, because a Relevant Person has no physical contact with the customer, the Relevant Person should obtain a copy certified as a true copy by a person of good standing such as a registered lawyer or notary, a chartered accountant, a bank manager, a police officer, an employee of the person's embassy or consulate, or other similar person. Downloading publicly-available information from an official source (such as a regulator or government website) is sufficient to satisfy the requirements of AML 6.3.1.(a) CDD information and research obtained from a reputable company or information-reporting agency may also be acceptable as a reliable and independent source, as would banking references and, for lower risk customers, information obtained from researching reliable and independent public information found on the internet or on commercial databases.

(e) For factors increasing the risk level, identification information is to be independently verified, using both public and non-public sources.

(f) In complying with AML 6.3.1.(c) a Relevant Person is required to "understand" a customer's source of funds. This means understanding where the funds for a particular service or transaction will come from (i.e. origin of funds used in carrying out a business transaction). The best way of understanding the source of funds is by obtaining information directly from the customer, which will usually be obtained during the on-boarding process. The Relevant Person should keep appropriate evidence of how they were able to understand the source of funds, for example, a copy of the customer account opening form, or customer onboarding form with confirmation of funds' initial sources taking into account customer's risk assessment and customer's behaviour in comparison with his/her risk profile.

(g) In complying with AML 6.3.1.(d) a Relevant Person is required to "understand" a customer's source of wealth. This means understanding the origin of the accumulated monetary assets of an individual, i.e. total assets. For a natural person, this might include information about thesource of wealth in an application form or customer questionnaire. The understanding should also be gained through interactions with the relationship manager at a financial institution. It could be gained by obtaining information from a reliable available source. The understanding need not be a dollar for dollar account of the customer's globalwealth, but it should provide sufficient detail to give the Relevant Person comfort that the customer's wealth is legitimate and also to provide a basis for subsequent on-going due diligence. The understanding of the customer's source of wealth may be clearly supported by title documents, for example, asset title document, audited financial statement, income tax return, etc. taking into account customer's risk assessment and customer's behaviour in comparison with his/her risk profile .

(h) Understanding a customer's sources of funds and wealth is also important for the purposes of creating customer risk profile and conducting on-going due diligence under AML 6.3.1.(e) Initial funding of an account or investments from an unknown or unexpected source may pose a money laundering risk. Similarly, a sound understanding of the customer's source of funds and wealth also provides useful information for a Relevant Person's transaction monitoring programme. Understanding of the customer's sources of funds or wealth shall be performed taking into account customer's risk assessment and customer's behaviour in comparison with his/her risk profile.

(i) An insurance policy which is similar to a life policy would include life-related protection, or a pension, or investment product which pays out to the policy holder or beneficiary upon a particular event occurring or upon redemption.

(j) A Relevant Person should conduct CDD in a manner proportionate to the customer's money laundering risks identified under Chapter 6. When the money laundering risks are identified as high, a Relevant Person must conduct EDD under Chapter 7.

(k) This means that all customers are subject to CDD under AML 6.3.1. However, for high risk customers, additional EDD measures should also be conducted under AML 7.1.1.

(l) The broad objective is that the Relevant Person should know at the outset of the relationship who its customers (and, where relevant, beneficial owners) are, where they operate, what they do and their expected level of activity. In addition to AML 6.1.1.(a), a Relevant Person must obtain documents on the legal form and the powers that regulate and bind the legal person or arrangement. The Relevant Person must then consider how the profile of the customer's financial behaviour builds up over time, allowing the Relevant Person to identify transactions or activity that may be suspicious.

Guidance on identification and verification of beneficial owners

(a) In determining whether an individual meets the definition of a beneficial owner or controller, regard should be had to all the circumstances of the case.

(b) When identifying beneficial owners, a Relevant Person is expected to adopt a substantive (as opposed to form over substance) approach to CDD for legal persons. Adopting a substantive approach means focusing on the money laundering risks of the customer and the product/service and avoiding an approach which focusses purely on the legal form of an arrangement or sets fixed percentages at which beneficial owners are identified (or not).

(c) A Relevant Person should take all reasonable steps to establish and understand a corporate customer's legal ownership and control and to identify the beneficial owner. An approach based only on defined thresholds without regard to the relevant risks in defining the beneficial owner may result in inadequate determination of beneficial ownership, for example, a criminal "gaming" the system by always keeping his financial interest below the relevant threshold.

A Relevant Person must consider a customer's risk rating and the source of funds when reviewing transactions as required by AML 6.4.1.

(d) In some circumstances no threshold should be used when identifying beneficial owners because it may be important to identify all underlying beneficial owners to ensure that they are not associated or connected in some way. This may be appropriate where there are a small number of investors in an account or fund, each with a significant financial holding and the customer-specific risks are higher. However, where the customer-specific risks are lower, a threshold can be appropriate. For example, for a low-risk corporate customer which, combined with a lower-risk product or service, a percentage threshold may be appropriate for identifying "control" of the legal person for the purposes of the definition of a beneficial owner.

(e) For a retail investment fund, which is widely-held and where the investors invest via pension contributions, the manager of the fund is not expected to look through to underlying investors where there are none with any material control or ownership levels in the fund. However, for a closely-held fund with a small number of investors, each with a large shareholding or other interest, a Relevant Person should identify and verify each of the beneficial owners, depending on the risks identified as part of its risk-based assessment of the customer.

(f) Where a Relevant Person carries out identification and verification in respect of actual and potential beneficial owners of a trust, the identification and verification should include the trustee, settlor, the protector, the enforcer, beneficiaries, other persons with power to appoint or remove a trustee and any person entitled to receive a distribution (whether or

not such person is a named beneficiary). For legal arrangements other than a trust, the identification and verification should include persons in positions similar to those in a trust exercising ultimate effective control over the legal arrangement (including through a chain of control or ownership) and entitled to receive a distribution (whether or not such person is a named beneficiary).

(g) A Relevant Person should identify and take reasonable measures to verify the identity of the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person to the extent that there is doubt under verification as to whether the person(s) with the controlling ownership interest is the beneficial owner(s). If no natural person exerts control through ownership interests, the Relevant Person should identify and take reasonable measures to verify the identity of the natural person(s) (if any) exercising control of the legal person or arrangement through other means.

(h) Where no natural person is identified as a beneficial owner who ultimately has a controlling ownership interest (or who has control through other means) in a legal person, the relevant natural person who holds the position of a member of senior management should be identified as such and verified.

Guidance on Politically Exposed Persons

(a) Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to a Relevant Person as their position may make them vulnerable to corruption. This risk also extends to members of their families and to their close (known) associates. PEP status itself does not incriminate individuals orentities. It does, however, put the customer into a high risk category until the EDD or on-going monitoring does not decrease the level of such risk.

(b) Generally, a PEP presents a higher risk of money laundering because there is a greater risk that such person, if he/she was committing money laundering, would attempt to place his/her money offshore where the customer is less likely to be recognised as a PEP and where it would be more difficult for law enforcement agencies in his/her home jurisdiction to confiscate or freeze his/her criminal property.

(c) Corruption-related money laundering risk increases when a Relevant Person deals with PEPs. Corruption may involve serious crimes and has become the subject of increasing global concern. Customer relationships with family members or close associates of PEPs involve similar risks to those associated with PEPs themselves.

(d) After leaving office PEPs may remain a higher risk for money laundering if they continue to exert political influence, directly or indirectly, or otherwise pose a risk of corruption.

6.4. On-going Customer Due Diligence

6.4.1. On-going obligation

When conducting on-going CDD under AML 6.3.1., a Relevant Person must, using the RBA:

(a) monitor and review transactions undertaken during the course of its customer relationship to ensurethat the transactions are consistent with the Relevant Person's knowledge of the customer, its business, its risk rating, and its source of funds;

(b) pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;

(c) enquire into the background and purpose of the transactions in paragraph (b) above;

(d) periodically review the adequacy of the CDD information it holds on customers and

beneficial owners to ensure that the information is kept up to date, particularly for customers with a high-risk rating;

(e) periodically review each customer to ensure that the risk rating assigned to a customer under AML 5.1.1.(b) remains appropriate for the customer in light of the money laundering risks; and

(f) at appropriate times apply CDD to existing customers based on materiality and risk considering whether and when CDD has been previously conducted and the adequacy of the CDD information obtained.

Guidance on on-going Customer Due Diligence

(a) In complying with AML 6.4.1. a Relevant Person should undertake a periodic review to ensure that non-static customer identity documentation is accurate and up-to-date. Examples of non-static identity documentation include passport number and residential/business address and, for a legal person, its share register or list of partners.

(b) A Relevant Person should undertake a review under AML 6.4.1.(d) particularly when:

(i) the Relevant Person changes its CDD documentation requirements;

(ii) an unusual transaction with the customer is expected to take place;

(iii) there is a material change in the business relationship with the customer; or

(iv) there is a material change in the nature or ownership of the customer.

(c) The degree of the on-going due diligence to be conducted will depend on the customer risk assessment carried out under AML 5.1.1.

(d) A Relevant Person's transaction monitoring policies, procedures, systems and controls, which may be implemented by manual or automated systems, or a combination of these, are one of the most important aspects of effective CDD. Whether a Relevant Person should undertake the monitoring by means of a manual or computerised system (or both) will depend on a number of factors, including:

(i) the size and nature of the Relevant Person's business and customer base; and

(ii) the complexity and volume of customer transactions.

6.5. Checking against sanctions and watchlists

6.5.1. Sanctions and Watchlists review

A Relevant Person must review its customers, their business and transactions against UNSC sanctions lists, Kazakhstan Sanctions List and Watchlists and any other lists of jurisdictions that they are obliged to follow with while establishing relationships and when complying with AML 6.4.1.(a), (d).

6.6. Failure to conduct or complete Customer Due Diligence

6.6.1. Prohibitions

Where, in relation to any customer, a Relevant Person is unable to conduct or complete the requisite CDD in accordance with AML 6.3.1. it must, to the extent relevant:

(a) not carry out a transaction with or for the customer through a bank account or in cash;

(b) not open an account or otherwise provide a service;

(c) not otherwise establish a business relationship or carry out a transaction;

(d) terminate any existing business relationship with the customer;

(e) [intentionally omitted]; and

(f) consider whether the inability to conduct or complete CDD necessitates the making of a STR (see Chapter 13).

A Relevant Person is prohibited from knowingly keeping anonymous accounts or accounts in obviously fictitious names.

6.6.2. Exceptions

A Relevant Person is not obliged to comply with AML 6.6.1.(a) to (e) if:

(a) to do so would amount to "tipping off" the customer, in contravention of the AML Law; or

(b) the FIU directs the Relevant Person to act otherwise.

Guidance on failure to conduct or complete Customer Due Diligence

(a) Where CDD cannot be completed, it may be appropriate not to carry out a transaction pending completion of CDD. Where CDD cannot be conducted, including where a material part of the CDD, such as identifying and verifying a beneficial owner cannot be conducted, a Relevant Person should not establish a business relationship with the customer.

(b) A Relevant Person should note that AML 6.6.1. applies to both existing and prospective customers. For new customers, it may be appropriate for a Relevant Person to terminate the business relationship before a product or service is provided. The Relevant Person should be careful not to "tip off" the customer.

(c) A Relevant Person should adopt the RBA for CDD of existing customers. For example, if a Relevant Person considers that any of its existing customers have not been subject to CDD at an equivalent standard to that required by these Rules, it should adopt the RBA and take remedial action in a manner proportionate to the risks and within a reasonable period of time whilst complying with AML 6.6.1.

7. ENHANCED DUE DILIGENCE

7.1. Conducting Enhanced Due Diligence

7.1.1. Obligation to conduct Enhanced Due Diligence

A Relevant Person must conduct EDD where money laundering risks are higher.

Where a Relevant Person is required to conduct EDD under AML 6.1.1. it must, to the extent applicable to the customer:

(a) obtain and verify additional:

(i) identification information on the customer and any beneficial owner;

(ii) information on the intended nature of the business relationship; and

(iii) information on the reasons for a transaction;

(b) update more regularly the CDD information which it holds on the customer and any beneficial owners;

(c) verify information on:

(i) the customer's SOF;

(ii) the customer's SOW;

(d) increase the degree and nature of monitoring of the business relationship, to determine whether the customer's transactions or activities appear unusual or suspicious;

(e) obtain the approval of senior management to commence a business relationship with a customer; and

(f) where applicable, require that any first payment made by a customer to open an account with a Relevant Person must be carried out through a bank account in the customer's name with:

(i) a bank;

(ii) a regulated Financial Institution whose entire operations are subject to regulation and supervision, including AML regulation and supervision, in a jurisdiction with AML regulations which are equivalent to the standards set out in the FATF Recommendations; or

(iii) a Subsidiary of a regulated Financial Institution referred to in (ii), if the law that applies to the parent ensures that the Subsidiary also observes the same AML standards as its parent.

Guidance on conducting Enhanced Due Diligence

(a) EDD measures are only mandatory to the extent that they are applicable to the relevant customer or the circumstances of the business relationship and to the extent that the risks would reasonably require it. Therefore, the extent of additional measures to conduct is a matter for the Relevant Person to determine on a case by case basis.

(b) For high risk customers, a Relevant Person should, in order to mitigate the perceived and actual risks, exercise a greater degree of diligence throughout the customer relationship

and should endeavour to understand the nature of the customer's businessand consider whether it is consistent and reasonable.

(c) A Relevant Person should be satisfied that a customer's use of complex legal structures and/or the use of trust and private investment vehicles, has a genuine and legitimate purpose.

(d) For EDD, where there is a beneficial owner, verification of the customer's source of funds and wealth may require enquiring into the beneficial owner's source of funds andwealth because the source of the funds would normally be the beneficial owner and notthe customer.

(e) Verification of sources of funds might include obtaining independent corroborating evidence such as proof of dividend payments connected to a shareholding, bank statements, salary/bonus certificates, loan documentation and proof of a transactionwhich gave rise to the payment into the account.

(f) A customer should be able to demonstrate and document how the relevant funds are connected to a particular event which gave rise to the payment into the account or to the source of the funds for a transaction.

(g) Verification of sources of wealth might include obtaining independent corroborating evidence such as share certificates, publicly-available registers of ownership, bank or brokerage account statements, probate documents, audited accounts and financial statements, news items from a reputable source and other similar evidence. For example:

(i) for a legal person, this might be achieved by obtaining its financial or annual reports published on its website or news articles and press releases that reflect itsfinancial situation or the profitability of its business; and

(ii) for a natural person, this might include documentary evidence which corroborates answers given to questions on the sources of wealth in an application form or customer questionnaire. For example, if a natural person attributes the source of his wealth to inheritance, he/she may be asked to provide a copy of the relevant will or grant of probate. In other cases, a natural person may be asked to provide sufficient bank or salary statements covering a number of years to draw up a picture of his/her sources of wealth.

(h) A Relevant Person might commission a third party report to obtain further information on a customer or transaction or to investigate a customer or beneficial owner in very high risk cases. A third party report may be particularly useful where there is little or no publicly-available information on a person or on a legal arrangement or where a Relevant Person has difficulty in obtaining and verifying information.

(i) In AML 7.1.1.(f) circumstances where it may be applicable to require the first payment made by a customer in order to open an account with a Relevant Person to be carried out through a bank account in the customer's name with a financial institution specified in AML 7.1.1.(f) include:

(i) where, following the use of other EDD measures, the Relevant Person is not satisfied with the results of due diligence; or

(ii) as an alternative measure, where one of the measures in AML 6.4.1. cannot be carried out.

8. SIMPLIFIED DUE DILIGENCE

8.1. Conduct of Simplified Due Diligence

8.1.1. Modifications to AML 6.3.1. for Simplified Due Diligence

Where a Relevant Person is permitted to conduct SDD under AML 6.1.2., modification of AML 6.3.1. may include:

(a) verifying the identity of the customer and identifying any beneficial owners after the establishment of the business relationship;

(b) deciding to reduce the frequency of, or as appropriate not undertake, customer identification updates;

(c) deciding not to verify an identified beneficial owner;

(d) deciding not to verify an identification document other than by requesting a copy;

(e) not enquiring as to a customer's SOF or SOW;

(f) reducing the degree of on-going monitoring of transactions, based on a reasonable monetary threshold or on the nature of the transaction; or

(g) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring such purpose and nature from the type of transactions or business relationship established.

8.1.2. Proportionality

The modification in AML 8.1.1. must be proportionate to the customer's money laundering risks.

Guidance on Simplified Due Diligence

(a) AML 8.1.1. provides examples of SDD measures. Other measures may also be used by a Relevant Person to modify CDD in accordance with the customer risks.

(b) A Relevant Person should not use a “one size fits all” approach for all its low risk customers. Notwithstanding that the risks may be low, the degree of CDD conducted needs to be proportionate to the specific risks identified on a case by case basis. For example, for customers where the money laundering risks are very low, a Relevant Person may decide simply to identify the customer and verify such information only to theextent that this is commercially necessary. On the other hand, a low risk customer which is undertaking a complex transaction might require more comprehensive procedures.

(c) For the avoidance of doubt, a Relevant Person is always required to identify beneficial owners, except for retail investment funds which are widely held, and investment funds where the investor invests via pension contributions. However, a Relevant Person may decide not to verify beneficial owners of a low risk customer.

(d) An example of circumstances where a Relevant Person might reasonably reduce the frequency of or, as appropriate, eliminate customer identification updates would be where the money laundering risks are low and the service provided does not offer a realistic opportunity for money laundering.

(e) An example of where a Relevant Person might reasonably reduce the degree of on-going

monitoring and scrutinising of transactions, based on a reasonable monetary threshold or on the nature of the transaction, would be where the transaction is a recurring, fixed contribution to a savings scheme, investment portfolio or fund or where the monetary value of the transaction is not material for money laundering purposes given the nature of the customer and the transaction type.

9. RELIANCE AND OUTSOURCING

9.1. Reliance on a third party

9.1.1. Permitted reliance

A Relevant Person may rely on the following third parties to conduct one or more elements of CDD on its behalf by entering into contractual agreement:

(a) an Authorised Person;

(b) a law firm, notary, or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent person in another jurisdiction;

(c) a Regulated Financial Institution; or

(d) a member of the Relevant Person's Group.

9.1.2. Reliance on information previously obtained

In AML 9.1.1., a Relevant Person may rely on the information previously obtained by a third party which covers one or more elements of CDD.

9.1.3. Extent of reliance

Where a Relevant Person seeks to rely on a person in AML 9.1.1., it may only do so if and to the extent that:

(a) it immediately obtains the necessary CDD information including customer and beneficial owner identification and verification documents, and information on the purpose and nature of the business relationship or transaction from the third party in AML 9.1.1.;

(a-a) the third parties in AML 9.1.1. have taken necessary measures within the scope of CDD, particularly, customer identification and record keeping;

(b) it takes adequate steps to satisfy itself that certified copies of the documents used to conduct the relevant elements of CDD will be available from the third party on request without delay. It is deemed sufficient that the third party certifies the customer identification documents as "the true copy of the original";

(b-a) regular assurance testing is carried out in respect of the third party arrangements, to ensure that the CDD documents can be retrieved without undue delay and that the documentation received is sufficient;

(c) the person in AML 9.1.1.(b) to (d) is subject to regulation, including AML regulation, by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations and it is supervised for compliance with such regulations;

(d) the person in AML 9.1.1. has not relied on any exception from the requirement to conduct any relevant elements of CDD which the Relevant Person seeks to rely on; and

(e) in relation to AML 9.1.2., the information is up to date.

9.1.4. Reliance on Group member

Where a Relevant Person relies on a member of its Group, such Group member need not meet the condition in AML 9.1.3.(c) if:

(a) the Group applies and implements a Group-wide policy on CDD and record keeping which

is equivalent to the standards set by the FATF;

(b) where the effective implementation of those CDD and record keeping requirements and AML programmes are supervised at Group level by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations; and

(c) the Group's AML policies adequately mitigate any high geographical risk factors.

9.1.5. Obligation to remedy deficiencies

If a Relevant Person is not reasonably satisfied that a customer or beneficial owner has been identified and verified by a third party in a manner consistent with these Rules, the Relevant Person must immediately perform the CDD itself with respect to any deficiencies identified.

9.1.6. Responsibility for compliance

Notwithstanding the Relevant Person's reliance on a person in AML 9.1.1., the Relevant Person remains responsible for compliance with, and liable for any failure to meet the CDD requirements in these Rules.

A Relevant Person must ensure that:

(a) a third party in AML 9.1.1. performed all appropriate CDD and record-keeping measures;

(b) the third party has an existing business relationship with the customer and that relationship is independent from the relationship to be formed by the customer with the Relevant Person; and

(c) the information provided by the third party satisfies the Relevant Person's own CDD requirements.

9.1.7 Prohibited reliance

(1) A Relevant Person must not rely on third parties to provide ongoing monitoring CDD procedures for its customers and counterparties on AML and sanctions matters.

(2) For the avoidance of doubt, reliance on third parties in this Rule does not apply to outsourcing or agency relationships established in accordance with AML 9.2. By relying to conduct one or more elements of CDD in outsourcing or agency relationship the Relevant Person is responsible for ensuring that ongoing due diligence is conducted on the business relationship and that transactions carried out in the course of that relationship are properly reviewed. The Relevant Person must ensure that customer's transactions are consistent with the Relevant Person's knowledge of the customer, its business and risk profile, including the source of funds.

Guidance on reliance

(a) [intentionally omitted]

(b) In complying with AML 9.1.3.(a) "immediately obtaining the necessary CDD information" means obtaining all relevant CDD information, and not just basic information such as name and address of the customer or beneficial owner. Compliance can be achieved by having that relevant information sentby fax, email or other appropriate means. For the avoidance of doubt, a Relevant Person is not required automatically to obtain the underlying certified documents used by the third party to conduct its CDD. A Relevant Person must, however, under AML 9.1.3.(b) ensure that the certified documents are readily available from the third party on request.

(c) A Relevant Person, in complying with AML 9.1.5., should fill any gaps in the CDD process

as soon as it becomes aware that a customer or beneficial owner has not been identified and verified in a manner consistent with these Rules.

(d) If a Relevant Person acquires another business, either in whole or in part, the Relevant Person may rely on the CDD conducted by the business it is acquiring but would expect the Relevant Person to have done the following:

(i) as part of its due diligence for the acquisition, to have taken a reasonable sample of the prospective customers to assess the quality of the CDD conducted; and

(ii) to conduct CDD on all the customers to cover any deficiencies identified in (i) as soon as possible following the acquisition, prioritising high risk customers.

(e) Where a jurisdiction's laws (such as secrecy or data protection legislation) would prevent a Relevant Person from having access to CDD information upon request without delay as referred to in AML 9.1.3.(b) the Relevant Person should conduct the relevant CDD itself and should not seek to rely on the relevant third party.

(f) If a Relevant Person relies on a third party located in another jurisdiction, including the Republic of Kazakhstan, to conduct one or more elements of CDD, the Relevant Person must ensure that such other jurisdiction has AML regulations that are equivalent to the standards set out in the FATF Recommendations (see AML 9.1.3.(c)).

(g) When assessing if AML regulations in another jurisdiction are equivalent to the FATF standards, a Relevant Person may consider a number of factors including, but not limited to: FATF membership, FATF Mutual Evaluation reports, FATF-style or IMF/World Bank evaluations, membership of an international or regional 'group', contextual factors such as political stability or the level of corruption, evidence of relevant criticism of a jurisdiction including FATF advisory notices or independent and public assessments of the jurisdiction's overall AML regime such as IMF/World Bank or other reports by reputable NGOs or specialized commercial agencies. A Relevant Person should, in making its assessment, rely only on sources that are up-to-date and that include the latest AML developments from a reliable and competent source. The assessment may also consider whether adequate arrangements exist for co-operation between the AML regulator in that jurisdiction and the AIFC. A Relevant Person must retain sufficient records of the sources and materials considered when undertaking this AML assessment.

9.2. Outsourcing

9.2.1. Responsibility for service providers

A Relevant Person which outsources any one or more elements of its CDD to a service provider (including within its Group) remains responsible for compliance with, and liable for any failure to meet, such obligations.

Guidance on outsourcing

A Relevant Person should conduct appropriate due diligence to assure itself of the suitability of a service provider and should ensure that the provider's obligations are clearly documented in a binding agreement.

For general requirements regarding outsourcing refer to GEN 5.2.

10. CORRESPONDENT BANKING

10.1. Application

10.1.1. Limits on application

This Chapter applies only to Authorised Persons.

10.2. Correspondent Banking

10.2.1. Obligations in respect of correspondent banking relationships

An Authorised Firm proposing to have a correspondent banking relationship with a respondent bank must:

(a) conduct appropriate CDD on the respondent bank;

(b) as part of (a), gather sufficient information about the respondent bank to understand fully the nature of the business, including making appropriate enquiries on its management, its major business activities and the countries or jurisdictions in which it operates;

(c) determine from publicly-available information the reputation of the respondent bank and the quality of supervision, including whether it has been subject to a money laundering investigation or relevant regulatory action;

(d) assess the respondent bank's AML controls and ascertain if they are adequate and effective in light of the FATF Recommendations;

(e) ensure that prior approval of the Authorised Firm's senior management is obtained before entering into a new correspondent banking relationship;

(f) understand the respective responsibilities of the parties to the correspondent banking relationship and properly document those responsibilities;

(g) be satisfied that, in respect of any customers of the respondent bank who have direct access to accounts of the Authorised Firm, the respondent bank:

(i) has conducted CDD (including on-going CDD) at least equivalent to that in AML 6.3.1. in respect of each customer;

(ii) will conduct ongoing CDD at least equivalent to that in AML 6.4.1., in respect of each customer; and

(iii) can provide the relevant CDD information in (i) to the Authorised Firm upon request; and

(h) document the basis for its satisfaction that the requirements in (a) to (g) are met.

In the process of completing the CDD, prior to establishing a correspondent banking relationship, the Authorised Firm must consider all of the following:

(a) whether it is regulated and supervised for AML and CFT purposes by a regulatory or governmental authority, body or agency equivalent to the Regulator in each foreign jurisdiction in which it operates;

(b) whether each foreign jurisdiction in which it operates has an effective AML and CFT regime;

(c) if the respondent is a subsidiary of another legal person—the following additional matters:

(i) the other person's domicile and location (if different);

(ii) its reputation;

(iii) whether the other person is regulated and supervised (at least for AML and CFT purposes) by a regulatory or governmental authority, body or agency equivalentto the Regulator in each jurisdiction in which it operates;

(iv) whether each foreign jurisdiction in which it operates has an effective AML and CFT regime;

(v) its ownership, control and management structure (including whether it is owned, controlled or managed by a politically exposed person).

If the Authorised Firm establishes a correspondent banking relationship with the respondent, the Authorised Firm must:

(a) conduct enhanced ongoing monitoring of the volume and nature of the transactions conducted under the relationship, and if necessary, obtain and record the information on the source of monies for conducted transactions; and

(b) conduct ongoing review of the relationship at least on an annual basis.

An Authorised Firm must:

(i) not enter into a correspondent banking relationship with a Shell Bank; and

(ii) take appropriate measures to ensure that it does not enter into, or continue a correspondent banking relationship with, a bank which is known to permit its accounts tobe used by Shell Banks.

Guidance on correspondent banking

AML 10.2.1. prohibits an Authorised Firm from entering into a correspondent banking relationship with a Shell Bank or a bank which is known to permit its accounts to be used by Shell Banks.

10.3. Prohibition of Shell Banks

A Shell Bank must not be established in, or operate in or from, the AIFC.

10.4. Pay Through Accounts

10.4.1. This rule applies if:

(a) a Bank (the *correspondent*) has a correspondent banking relationship with a financial institution (the *respondent*) in a foreign jurisdiction; and

(b) under the relationship, a customer of the respondent who is not a customer of the correspondent may have direct access to an account of the correspondent.

(1) The Bank (correspondent) must not allow any of the customers of the respondent to have access to the account of any of its own customers, unless the correspondent is satisfied that the respondent:

(a) has conducted CDD measures for all of its customers and verified their identity;

(b) conducts ongoing monitoring for its customers; and

(c) can provide to the correspondent, on request, the documents, data and information obtained in conducting CDD and ongoing monitoring for any of its customers.

(2) In the event of the correspondent asking the respondent for documents, data or information mentioned in (c) above and the respondent fails to satisfactorily comply with the request, the correspondent must immediately terminate the customer's access to accounts of the correspondent and consider making a STR to the FIU.

10.5. Payment processing using On-line services

10.5.1. Electronic verification of identification documentation

An Authorised Firm may rely on electronic verification of identification documentation if it complies with the RBA and other requirements of these Rules.

An Authorised Firm must make and keep a record that clearly demonstrates the basis on which it relies on the electronic verification of identification documentation.

An Authorised Firm may permit payment processing to take place using on-line services if it ensures that the processing is subject to:

(a) the same monitoring as its other services; and

(b) the same risk-based methodology.

11. WIRE TRANSFERS

11.1. Definitions

11.1.1. Defined terms

In this Chapter:

(a) "beneficiary institution" means the Financial Institution that receives the wire transfer from the ordering institution, whether directly or through an intermediary institution, and makes the funds available to the payee;

(b) "cover payment" means a wire transfer that combines a payment message sent directly by the ordering institution to the beneficiary institution with the routing of the funding instruction from the ordering institution to the beneficiary institution through one or more intermediary institutions;

(c) "cross-border wire transfer" means a wire transfer where the ordering institution and the beneficiary institution are located in different jurisdictions and includes any chain of wire transfers in which at least one of the Financial Institutions involved is located in a different jurisdiction;

(d) "customer identification number" means a number that is different from the unique transaction reference number and:

(i) uniquely identifies the payer to the ordering institution; and

(ii) refers to a record held by the ordering institution that contains at least one of the following: the payer's address, national identity number or date and place of birth;

(e) "domestic wire transfer" means a wire transfer where the ordering institution and beneficiary institution are located in the same jurisdiction and includes any chain of wire transfers that takes place entirely within a jurisdiction, even if the system used to transfer the payment message is located in another country;

(f) "intermediary institution" means the Financial Institution in a serial payment or cover payment chain that receives and transmits a wire transfer on behalf of the ordering institution and the beneficiary institution, or another intermediary institution;

(g) "ordering institution" means the Financial Institution that transfers the funds upon receiving the request for a wire transfer on behalf of the payer;

(h) "payee" means the natural or legal person or legal arrangement identified by the payer as the recipient of the requested wire transfer;

(i) "payer" means the account holder or originator who allows/instructs the wire transfer from that account or, if there is no account, the natural or legal person that places the wire transfer order with the ordering institution to perform the wire transfer;

(j) "serial payment" means a direct sequential chain of payment where the wire transfer and accompanying payment message travel together from the ordering institution to the beneficiary institution, directly or through one or more intermediary institutions;

(k) "straight-through processing" means payment transactions that are conducted electronically without the need for manual intervention;

(l) "unique transaction reference number" means a combination of letters, numbers or symbols, determined by the Financial Institution in accordance with the protocols of the payment and settlement system or messaging system used for the wire transfer, and which permits the traceability of the wire transfer; and

(m) "wire transfer" includes any value transfer process or arrangement.

11-1. TRANSFER OF DIGITAL ASSETS

11-1.1. Digital Asset transfer

(1) If a Digital Asset Service Provider transfers Digital Assets to another Digital Asset Service Provider:

the originating Digital Asset Service Provider must:

(i) obtain and hold required and accurate originator information and required beneficiary information on the transfer; and

(ii) immediately and securely submit the information in (i) to the beneficiary Digital Asset Service Provider or any other relevant institution as so required by law.

(2) The information in (1) should be stored in a manner such that it cannot be altered and so that it is readily available to AFSA on AFSA's request.

(3) For the purposes of 1(a), an originating Digital Asset Service Provider must ensure that all transfers of Digital Assets with value equal to or more than USD1,000 involving natural persons are accompanied by:

(a) the name of the originator;

(b) the originator's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number;

(c) the originator's physical address, or national identity number, or customer identification, or date and place of birth;

(d) the name of the beneficiary; and

(e) the beneficiary's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number.

(4) For the purposes of 1(a), an originating Digital Asset Service Provider must ensure that all transfers of Digital Assets with value equal of less than USD 1,000 involving natural persons are accompanied by:

(a) the name of the originator;

(b) the originator's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number;

(c) the name of the beneficiary; and

(d) the beneficiary's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number.

(5) For the purposes of 1(a), an originating Digital Asset Service Provider must ensure that all all transfers of Digital Assets with value equal to or more than USD 1,000 involving Body Corporates are accompanied by:

(a) the registered corporate name or trading name of the originator;

(b) the originator's digital asset wallet address or account number or (in the absence of an account) unique transaction reference number;

(c) either of the following:

(i) the customer identification number; or

(ii) the registered office address or primary place of business;

(d) the following beneficiary information:

(i) the name of the beneficiary; and

(ii) beneficiary's digital asset wallet address account number or (in the absence of an account) unique transaction reference number.

(6) For the purposes of 1(a), an originating Digital Asset Service Provider must ensure that all transfers of Digital Assets with value equal of less than USD 1,000 involving Body Corporates are accompanied by:

(a) the name of the originator;

(b) the originator's account number or (in the absence of an account) unique transaction reference number;

(c) the following required beneficiary information;

(i) the name of the beneficiary; and

(ii) beneficiary's account number or (in the absence of an account) unique transaction reference number.

(7) The Digital Asset Service Provider should not execute a transaction if it does not comply with requirements set out in (3), (4), (5) or (6), as applicable, and should return the relevant amounts back to the originator. The Digital Asset Service Provider should have appropriate risk-based policies and procedures to determine when to execute, reject or suspend a transfer lacking the required information while at all times complying with these requirements.

(8) In determining the value of a transfer, Digital Asset Service Providers must take a reasonable and justified approach. If multiple transfers from the same originator appear to be linked, they will be aggregated for the purpose of calculating the transfer's value.

(9) An intermediary Digital Asset Service Provider who participates in transfers of Digital Assets must:

(a) take reasonable measures, consistent with current guidance, to identify transfers of Digital Assets that lack the required originator or beneficiary information;

(b) adopt risk-based policies and procedures to determine when to execute, reject or suspend a transfer lacking the required information; and

(c) keep records for at least 6 years after the completion of the transaction to which it relates.

(10) If several transfers from a single originator are bundled in a batch file for transmission to beneficiaries, they may be exempted from the requirements in respect of originator information, provided that they include the originator's account number or unique transaction reference number, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

11-1.2. Digital Asset Transfers to or from self-hosted digital wallets

(1) In case of a transfer of a Digital Asset made to or received from a self-hosted digital wallet, the Digital Asset Service Provider of the originator or beneficiary must obtain and hold information referred to in 11-1.1.(3), (4), (5) or (6) from Clients and ensure that the transfer of Digital Assets can be individually identified.

(2) If a Digital Asset transfer exceeds USD 1,000 or there is a suspicion of money laundering or terrorist financing of a transfer to a self-hosted digital wallet, the Digital Asset Service Provider of the originator or beneficiary must take adequate measures on a risk-sensitive basis to mitigate and manage the money laundering and terrorist financing risks associated with the transfer.

Guidance on risk mitigating measures on transfers to or from self-hosted digital wallets

A Digital Asset Service Provider should undertake the following non-exhaustive measures to ensure compliance with AML 11-1.2 (2):

(a) to conduct enhanced monitoring of Digital Asset transfers with self-hosted digital wallets;

(b) to accept Digital Asset transfers from or to self-hosted digital wallets only where the Digital Asset Service Provider has them assessed to be reliable, having regard to the screening results of the Digital Asset transactions and the associated digital wallets and the assessment results on the ownership or control of the self-hosted digital wallet by the originator or beneficiary; and

(c) to impose transaction limits or prohibition.

Note: Chapter 11-1. comes into operation 12 months after the commencement date of the AIFC Rules on Digital Asset Activities.

11-2. DIGITAL ASSET TRANSFER COUNTERPARTY DUE DILIGENCE AND ADDITIONAL MEASURES

11-2.1. General requirements

(1) If a Digital Asset Service Provider conducts a Digital Asset transfer referred to in Chapter 11-1, the Digital Asset Service Provider will be exposed to money laundering and terrorist financing risks associated with the institution which may be the ordering institution, intermediary institution or

beneficiary institution involved in the Digital asset transfer ("Digital Asset transfer counterparty").

(2) To avoid sending or receiving a Digital Asset to or from illicit actors or designated parties that had not been subject to appropriate CDD and screening measures of a Digital Asset transfer counterparty and to ensure compliance with the Travel Rule, a Digital Asset Service Provider must conduct due diligence on the Digital Asset transfer counterparty. A Digital Asset Service Provider should identify and assess the money laundering and terrorist financing risks associated with the Digital Asset transfer to or from the Digital Asset transfer counterparty and apply the appropriate risk-based anti-money laundering and countering financing terrorism measures.

(3) A Digital Asset Service Provider must conduct due diligence measures on a Digital Asset transfer counterparty before conducting a Digital Asset transfer or making the transferred Digital Assets available to the recipient.

(4) A Digital Asset Service Provider does not need to undertake the Digital Asset transfer counterparty due diligence process for every individual Digital Asset transfer when dealing with Digital Asset transfer counterparties that it has already conducted counterparty due diligence on previously, unless there is a suspicion of money laundering and terrorist financing.

(5) A Digital Asset Service Provider must undertake reviews of the Digital Asset transfer counterparty due diligence records on a regular basis or upon trigger events (e.g., when it becomes aware of a suspicious transaction or other information such as negative news from credible media, public information that the counterparty has been subject to any targeted financial sanction, money laundering and terrorist financing investigation or regulatory action).

(6) Based on the Digital Asset transfer counterparty due diligence results, a Digital Asset Service Provider must determine if it should continue to conduct Digital Asset transfers with, and submit the required information to, a Digital Asset transfer counterparty, and the extent of anti-money laundering and countering financing terrorism measures that it should apply in relation to a Digital Asset transfer with the Digital Asset transfer counterparty on a risk-sensitive basis.

Guidance

Digital Asset transfer counterparty due diligence may involve the following non-exhaustive procedures:

(a) determining whether a Digital Asset transfer is or will be with a Digital Asset transfer counterparty or a self-hosted digital wallet;

(b) where applicable, identifying the Digital Asset transfer counterparty (e.g., by making a reference to a list of licensed or registered Digital Asset Service Providers or financial institutions in different jurisdictions); and

(c) assessing whether a Digital Asset transfer counterparty is an eligible counterparty to deal with and to send the required information to.

11-2.2. Digital Asset transfer counterparty due diligence measures

A Digital Asset Service Provider must apply the following Digital Asset transfer counterparty due diligence measures before it conducts a Digital Asset transfer with a Digital Asset transfer counterparty:

(a) determining if the respondent entity is licensed or registered;

(b) collecting sufficient information about the Digital Asset transfer counterparty to enable it to understand fully the nature of the Digital Asset transfer counterparty's business;

(c) understanding the nature and expected volume and value of a Digital Asset transfer with the Digital Asset transfer counterparty;

(d) determining from publicly available information the reputation of the Digital Asset transfer counterparty and the quality and effectiveness of the anti-money laundering and countering financing terrorism regulation and supervision over the Digital Asset transfer counterparty by authorities in the relevant jurisdiction;

(e) assessing the anti-money laundering and countering financing terrorism controls of a Digital Asset transfer counterparty and ensure that they are adequate and effective;

(f) assessing whether the Digital Asset transfer counterparty is subject to the Travel Rule similar to that imposed under Chapter 11-1 in the jurisdiction in which the Digital Asset

transfer counterparty operates or is incorporated;

(g) assessing the adequacy and effectiveness of the anti-money laundering and countering financing terrorism controls that the Digital Asset transfer counterparty has put in place for ensuring compliance with the Travel Rule;

(h) assessing whether the Digital Asset transfer counterparty can protect the confidentiality and integrity of personal data (e.g., the required originator and recipient information), taking into account the adequacy and robustness of data privacy and security controls of the Digital Asset transfer counterparty; and

(i) obtaining approval from its senior management.

Guidance:

(1) While a relationship with a Digital Asset transfer counterparty is different from a cross-border correspondent relationship referred to in Chapter 10, there are similarities in the due diligence approach which can be of assistance to a Digital Asset Service Provider. By virtue of this, the Digital Asset Service Provider should conduct due diligence measures in Chapter 10, with reference to the requirements set out in AML 10.2.

(2) When assessing money laundering and terrorist financing risks posed by a Digital Asset transfer counterparty, a Digital Asset Service Provider should take into account the relevant factors that may indicate a higher money laundering and terrorist financing risk. Examples of such risk are where a Digital Asset transfer counterparty:

(i) operates or is incorporated in a jurisdiction posing a higher risk or with a weak anti-money laundering and countering financing terrorism regime;

(ii) is not (or yet to be) licensed or registered and supervised for anti-money laundering and countering financing terrorism purposes in the jurisdiction in which it operates or is incorporated by the relevant authorities;

(iii) does not have in place adequate and effective anti-money laundering and countering financing terrorism systems, including measures for ensuring compliance with the Travel Rule;

(iv) does not implement adequate measures or safeguards for protecting the confidentiality and integrity of personal data; or

(v) is associated with money laundering and terrorist financing or other illicit activities.

Note: Chapter 11-2. comes into operation 12 months after the commencement date of the AIFC Rules on Digital Asset Activities.

11.2. Wire transfer requirements

11.2.1. Obligations in respect of wire transfer

An Authorised Person must:

(a) when it sends or receives funds by wire transfer on behalf of a customer ensure that the wire transfer and any related messages contain payer and payee information;

(b) monitor wire transfers for the purpose of detecting those wire transfers that do not contain payer and payee information and take appropriate measures to identify any money laundering risks;

(c) where there is a suspicion of money laundering:

(i) conduct CDD when carrying out transactions, including occasional transactions, that are wire transfers (cross-border wire transfers and domestic wire transfers, including

serial payments, and cover payments); and

(ii) verify the information pertaining to its customer.

11.2.2. Financial Institutions acting on their own behalf

The requirement in AML 11.2.1. does not apply to Financial Institution-to-Financial Institution transfers and settlements, where both the payer and the payee are Financial Institutions acting on their own behalf.

11.2.3. Requirements for ordering institutions

(a) An Authorised Person must ensure that information accompanying all cross-border wire transfers less than USD 1,000 contains:

(i) the name of the payer:

(ii) the payer account number where such an account is used to process the transaction (or unique transaction reference number that allows traceability of the transaction if no account exists);

(iii) the name of the payee; and

(iv) the payee account number where such an account is used to process the transaction (or unique transaction reference number that allows traceability of the transaction if no account exists).

(b) For all cross-border wire transfers of USD 1,000 or more an Authorised Person must ensure that, in addition to the information required by AML 11.2.3.(a), there is information containing the payer's address or national identity number (individual identification number or passport number), or customer identification number, or date and place of birth.

(c) If several individual cross-border wire transfers from a single payer are bundled in a batch file for transmission to payees, then an Authorised Person that is an ordering institution must ensure that:

(i) the batch file contains the payer information required under (a) and (b);

(ii) it has verified the payer information referred to in (i); and

(iii) the batch file contains the payee information required under (a) for each payee and that information is fully traceable in each payee's jurisdiction.

(d) For a domestic wire transfer, an Authorised Person that is an ordering institution must either:

(1) include in the information accompanying the wire transfer the following:

(i) the name of the payer;

(ii) the payer's account number where such an account is used to process the transaction (or unique transaction reference number that allows traceability of the transaction if no account exists); and

(iii) payer's address or national identity number (individual identification number or passport number), or customer identification number, or date and place of birth; or

(2) if the payer information set out in (1) can be given by other means, include the payer's account number or unique transaction reference number if no account exists, provided that:

(i) either number will permit the transaction to be traced back to the payer or the payee; and

(ii) the ordering institution must provide the payer information set out in paragraph (1) within 3 business days of a request for the information by the

beneficiary institution or the AFSA or immediately upon request of a law enforcement agency.

(e) An Authorised Person that is an ordering institution must maintain, in accordance with AML 14.5., a record of the payer and payee information it has collected under this Chapter.

(f) An Authorised Person that is an ordering institution must not perform a wire transfer if it is unable to comply with the requirements in AML 11.2.3.

Guidance on wire transfers

(a) [intentionally omitted]

(b) Concealing or removing in a wire transfer any of the information required by AML 11.2.1. would be a contravention of the requirement to ensure that the wire transfer contains payer and payee information.

(c) The information required under AML 11.2.3.(a) for all cross-border wire transfers less than USD 1,000 need not be verified for accuracy except if the Relevant Person suspects money laundering.

11.2.4. Requirements for intermediary institution

(a) An Authorised Person that is an intermediary institution must maintain all the required payer and payee information accompanying the wire transfer.

(b) If technical limitations prevent the required payer or payee information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, an Authorised Person that is a receiving intermediary institution must maintain a record, for at least six years, of all the information received from the ordering institution or another intermediary institution.

(c) An Authorised Person that is an intermediary institution must take reasonable measures, which are consistent with straight-through processing, to identify cross-border wire transfers that lack the required payer or payee information.

11.2.5. Requirements for beneficiary institution

(a) An Authorised Person that is a beneficiary institution must take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack the required payer or payee information.

(b) For a cross-border wire transfer of USD 1,000 or more, an Authorised Person that is a beneficiary institution must verify the identity of the payee, if the identity has not been previously verified, and maintain this information in accordance with AML 14.5.

11.2.6. Systems and controls concerning wire transfers

An Authorised Person that acts as an intermediary or beneficiary institution must develop, establish and maintain policies, procedures, systems and controls to determine:

(a) when to perform, reject or suspend a wire transfer that lacks the full payer information or required payee information; and

(b) when to take an appropriate follow-up action.

11.2.7. Money or value transfer service operator

(a) An Authorised Person that is a money or value transfer service operator must comply with

all of the relevant requirements of AML 11.2. in the jurisdictions in which they operate, directly or through their agents.

(b) In the case of an Authorised Person that is a money or value transfer service operator that controls both the ordering and the payee side of a wire transfer, an Authorised Person must:

(i) take into account all the information from both the ordering and payee sides in order to determine whether a STR has to be filed; and

(ii) file a STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the FIU.

12. SANCTIONS

12.1. Relevant resolutions and sanctions

12.1.1. Sanctions systems and controls

A Relevant Person must establish and maintain effective systems and controls to ensure that on an on-going basis it is properly informed as to, and takes reasonable measures to comply with, relevant resolutions or sanctions issued by the UNSC, by the Republic of Kazakhstan, or with other sanctions applicable in the AIFC.

A Relevant Person must comply with prohibitions from conducting transactions with designated persons and entities, in accordance with the obligations set out in the relevant resolutions or sanctions issued by the UNSC, by the Republic of Kazakhstan or by other jurisdictions as applicable in the AIFC[2].

A Relevant Person must freeze without delay and without prior notice,the funds or other assets of designated persons and entities pursuant to relevant resolutions or sanctions issued by the UNSC or by the Republic of Kazakhstan.

12.1.2. Notification obligation

A Relevant Person must report to the FIU any assets frozen or actions taken in compliance with the prohibition requirements of the relevant resolutions or sanctions issued by the UNSC or by the Republic of Kazakhstan, including attempted transactions.

A Relevant Person must immediately notify the AFSA when it becomes aware that it is:

(a) carrying on or about to carry on an activity;

(b) holding or about to hold money or other assets; or

(c) undertaking or about to undertake any other business whether or not arising from or in connection with (a) or (b),

for or on behalf of a person, where such carrying on, holding or undertaking constitutes or may constitute a contravention of a relevant sanction or resolution issued by the UNSC or by the Republic of Kazakhstan.

12.1.2-1. A Relevant Person must report to the AFSA any actions taken regarding the customer in compliance with the prohibition requirements of the relevant resolutions or sanctions.

12.1.3. Notification requirements

A Relevant Person must ensure that the notification stipulated in AML 12.1.2. and 12.1.2-1. above includes thefollowing information:

(a) a description of the relevant activity in AML 12.1.2.; and

(b) the action proposed to be taken or that has been taken by the Relevant Person regarding the matters specified in the notification.

Guidance on sanctions

(a) In AML 12.1.1. taking reasonable measures to comply with a resolution or sanction may mean that a Relevant Person cannot undertake a transaction for or on behalf of a person

[2] List of financial sanctions applicable in the AIFC is presented in the Practical Guidance to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework.

or that it may need to conduct further due diligence in respect of a person.

(b) Relevant resolutions or sanctions mentioned in AML 12.1.1. may, among other things, relate to money laundering, sanctions violation or otherwise be relevant to the activities carried on by the Relevant Person.

(c) A Relevant Person should exercise due care to ensure that it does not provide services to, or otherwise conduct business with, a person engaged in money laundering and sanctions violation.

(d) When making a notification to the AFSA in accordance with AML 12.1.2., a Relevant Person should have regard to the requirements of the AML Law in relation to freezing assets and blocking transactions and must also consider whether itis necessary to file a STR.

(e) An Authorised Market Institution should exercise due care to ensure that it does not facilitate fund raising activities or listings by persons engaged in money laundering or sanctions violation.

(f) Relevant Persons must perform checks on an on-going basis against their customer databases and records for any names appearing in resolutions or sanctions as well as to monitor transactions accordingly.

(g) A Relevant Person may use a database maintained elsewhere for an up-to-date list of resolutions and sanctions, or to perform checks of customers or transactions against that list. For example, it may wish to use a database maintained by its head office or a Group member. However, the Relevant Person retains responsibility for ensuring that its systems and controls are effective to ensure compliance with these Rules.

12.2. Government, Regulatory and International Findings

12.2.1. Compliance with Findings

A Relevant Person must establish and maintain systems and controls to ensure that on an on-going basis it is properly informed as to, and takes reasonable measures to comply with, any findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions (each of which is referred to in this Rule as a "Finding") issued by (as applicable):

(a) the government of the Republic of Kazakhstan;

(b) the National Bank of the Republic of Kazakhstan;

(c) Agency of Financial Monitoring of the Republic of Kazakhstan;

(d) the AFSA; and

(e) the FATF,

concerning the matters in AML 12.2.2.

12.2.2. Relevant matters

For the purposes of AML 12.2.1., the relevant matters are:

(a) arrangements for preventing money laundering in a particular country or jurisdiction, including any assessment of material deficiency against relevant countries in adopting international standards; and

(b) the names of persons, groups, organisations or entities or any other body where suspicion of money laundering exists.

12.2.3. Notification obligations

A Relevant Person must immediately notify the AFSA in writing if it becomes aware of non-compliance by a person with a Finding and provide the AFSA with sufficient details of the person concerned and the nature of the non-compliance.

12.2.4 Additional measures

A Relevant Person should be able to independently apply countermeasures that are effective, appropriate and proportionate (including EDD measures) to AML and CFT risks, whether or not called upon to do so for the purposes of AML 12.2.1., including by the FATF.

Guidance on Government, Regulatory and International Findings

(a) The purpose of these Rules is to ensure that a Relevant Person takes into consideration the broad range of tools used by competent authorities and international organisations to communicate AML and CFT risks to stakeholders.

(b) A Relevant Person should examine and pay special attention to any transactions or business relationship with persons located in countries or jurisdictions mentioned by the entities in AML 12.2.1.(a) to (e).

(c) Relevant Persons considering transactions or business relationships with persons located in countries or jurisdictions that have been identified as deficient, or against which the Republic of Kazakhstan or the AFSA have outstanding advisories, should be aware of the background against which the assessments, or the specific recommendations have been made. These circumstances should be taken into account in respect of introduced business from such jurisdictions, and when receiving inward payments for existing customers or in respect of inter-bank transactions.

(d) The Relevant Person's MLRO is not obliged to report all transactions from these countries or jurisdictions to the Kazakhstan state agencies if they do not qualify as suspicious. See Chapter 13 on STRs.

(e) Transactions with counterparties located in countries or jurisdictions which have been but are no longer identified as deficient or have been relieved from special scrutiny may nevertheless require attention which is higher than normal.

(f) In order to assist Relevant Persons, the AFSA will, from time to time, publish findings, guidance, directives, or sanctions made by FATF, the UNSC, or the government of the Republic of Kazakhstan. However, a Relevant Person must take its own steps to acquire relevant information from various available sources. For example, a Relevant Person may obtain relevant information from the FIU, European Union, the United Kingdom (HM Treasury) lists, and the United Statesof America (Office of Foreign Assets Control of the Department of Treasury).

(g) In addition, the systems and controls set out in AML 12.1.1. should be established and maintained by a Relevant Person, taking into account the risk assessments under Chapters 5 and 6. In AML 12.1.1., taking reasonable measures to comply with a finding may mean that a Relevant Person cannot undertake a transaction for or on behalf of a person or that it may need to conduct further due diligence in respect of such a person.

(h) A Relevant Person should be proactive in obtaining and appropriately using available national and international information, for example, suspect lists or databases from credible public or private sources regarding money laundering, including obtaining relevant information from sources mentioned in (f) above. Relevant Persons should perform checks against their customer databases and records for any names appearing on such lists and databases as well as to monitor transactions accordingly. As set out in the Guidance, a Relevant Person may use a database maintained elsewhere for an up-to date list of sanctions or to conduct checks of customers or transactions against the list.

However, it retains responsibility for ensuring the effectiveness of its systems and controls

(i) The risk of terrorists entering the financial system can be reduced if Relevant Persons apply effective AML strategies, particularly in respect of CDD. Relevant Persons should assess which countries carry the highest risks and should conduct an analysis of transactions from countries or jurisdictions known to be a source of terrorist financing.

(j) The AFSA may require Relevant Persons to take any special measures it may prescribe with respect to certain types of transactions or accounts where the AFSA reasonably believes that any of the above may pose a risk of money laundering.

13. MONEY LAUNDERING REPORTING OFFICER, THRESHOLD TRANSACTIONS, SUSPICIOUS TRANSACTIONS AND TIPPING OFF

13.1. Money Laundering Reporting Officer

13.1.1. Who can act as Money Laundering Reporting Officer

The MLRO function must be carried out by an individual who has responsibility for the implementation and oversight of an Authorised Person's AML policies, procedures, systems and controls and can act independently in this role.

If MLRO function is carried out solely, it must be carried out by an individual who is at an appropriate level of seniority (for example, at the same level of authority as a Director, Partner, Principal Representative, or Senior Manager of an Authorised Person).

If MLRO function is carried out as a special function delegated by a Compliance Officer to a designated individual (MLRO), then such individual's independence in decision-making must be preserved[3].

13.1.2. Appointment of Money Laundering Reporting Officer

A Relevant Person must appoint an individual as MLRO, with responsibility for implementation and oversight of its compliance with the AML Rules, who has an appropriate level of seniority and independence to act in the role.

An Authorised Firm, other than a Representative Office, must appoint an individual to act as a deputy MLRO of the Authorised Firm to fulfil the role of the MLRO in his or her absence.

13.1.3. Residency Requirement

The MLRO must be resident in the Republic of Kazakhstan except in the case of the MLRO for a Registered Auditor.

Guidance on appointment of Money Laundering Reporting Officer

(a) Under GEN 2.1.2., the MLRO function is a mandatory appointment.

(b) A Relevant Person other than an Authorised Firm should make adequate arrangements to ensure that it remains in compliance with these Rules in the event that its MLRO is absent. Adequate arrangements would include appointing a temporary MLRO for the period of the MLRO's absence or making sure that the Relevant Person's AML systems and controls allow it to continue to comply with these Rules when the MLRO is absent.

13.2. [Intentionally omitted]

13.2.1. [Intentionally omitted]

13.3. Dealing with the Regulator

13.3.1. Obligation of co-operation

A Relevant Person's MLRO must deal with the AFSA in an open, responsive, and co-operative manner and must disclose appropriately any information of which the AFSA would reasonably be expected to be notified.

13.4. Outsourcing the role of Money Laundering Reporting Officer

[3] Additional clarification is presented in the Practical Guidance to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework.

13.4.1. Outsourcing permitted

A Relevant Person may outsource the role of MLRO to an individual outside the Relevant Person if the relevant individual under the outsourcing agreement is and remains suitable to perform the MLRO role.

13.4.2. Responsibility for compliance

Where a Relevant Person outsources specific AML tasks of its MLRO to another individual or a third-party provider, including within a corporate Group, the Relevant Person remains responsible for ensuring compliance with the responsibilities of the MLRO. The Relevant Person should satisfy itself of the suitability of anyone who acts for it.

13.5. Qualities of Money Laundering Reporting Officer

13.5.1. Organisational standing

A Relevant Person must ensure that its MLRO has:

(a) direct access to its senior management;

(b) a level of seniority and independence within the Relevant Person to enable him/her to act on his/her own authority and to act independently in carrying out his/her responsibility;

(c) sufficient resources, including appropriate staff and technology; and

(d) timely and unrestricted access to information sufficient to enable him/her to carry out his/her responsibilities in AML 13.6.1.

Guidance on qualities of Money Laundering Reporting Officer

A Relevant Person will need to consider AML 13.5.1. when appointing an outsourced MLRO. Any external MLRO that is appointed will need to have the actual or effective level of seniority that the role requires.

13.6. Responsibilities of Money Laundering Reporting Officer

13.6.1. Oversight responsibility

A Relevant Person must ensure that its MLRO implements and has oversight of, and is responsible for, the following matters:

(a) the day-to-day operations for compliance by the Relevant Person with its AML policies, procedures, systems and controls;

(b) acting as the point of contact to receive notifications from the Relevant Person's employees under AML 13.7.3.;

(c) taking appropriate action under AML 13.8.1. following the receipt of a notification from an employee;

(d) ensuring that the STRs and TTRs are sent to the FIU in accordance with applicable Kazakhstan law;

(e) acting as the point of contact within the Relevant Person for the AFSA, and anyother competent authority regarding money laundering issues;

(f) responding promptly to any request for information made by the AFSA, and anyother competent authority;

(g) receiving and acting upon any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in Chapter 12;

(h) establishing and maintaining an appropriate money laundering training programme and adequate awareness arrangements under Chapter 14; and

(i) preparing conclusions based on the results of CDD and make decisions on the possibility of establishing relations with the client, except in cases stipulated by AML 6.3.3.(b).

13.7. Reporting

A Relevant Person must complete the AFSA's AML Return form on an annual basis and submit such form to the AFSA within two months after the end of each year;

13.7.1. Defined terms

In this Chapter, a reference to a criminal offence for “money laundering” is as set out in the Kazakhstan criminal law.

13.7.2. Threshold Transactions Controls

A Relevant Person must establish and maintain policies, procedures, systems and controls to monitor and detect transactions above defined thresholds, and submit threshold transactions reports (“TTRs”) to the FIU in accordance with the AML Law.

13.7.3. Suspicious Activity and Transactions Controls

A Relevant Person must establish and maintain policies, procedures, systems and controls to monitor and detect suspicious activity or transactions in relation to potential money laundering.

A Relevant Person must register in the FIU reporting system for submitting STRs or TTRs before the commencement of its business activities.

13.7.4. Immunity from liability for disclosure of information relating to money laundering transactions

(a) The disclosure by a Relevant Person to the competent authorities of information relating to money laundering is not a contravention of any obligation of secrecy or non-disclosure or (where applicable) of any enactment by which that obligation is imposed.

(b) The sharing by the Authorised Persons where this is required by Chapters 9, 10 and 11 of information relating to money laundering is not a contravention of any obligation of financial institution secrecy laws or non-disclosure or (where applicable) of any enactment by which that obligation is imposed.

13.7.5. Employee reporting to Money Laundering Reporting Officer

A Relevant Person must have policies, procedures, systems and controls to ensure that whenever any employee, acting in the ordinary course of his employment, either:

(a) knows;

(b) suspects; or

(c) has reasonable grounds for knowing or suspecting,

that a person is engaged in or attempting money laundering, that employeepromptly notifies the Relevant Person’s MLRO and provides the MLRO with all relevant information within the employee's knowledge.

Guidance on Suspicious Transaction Reports

(a) Circumstances that might give rise to suspicion or reasonable grounds for suspicion include:

(i) Transactions which have no apparent purpose, which make no obvious economic sense, or which are designed or structured to avoid detection;

(ii) Transactions requested by a person without reasonable explanation, which are out of the ordinary range of services normally requested or are outside the experience of a Relevant Person in relation to a particular customer;

(iii) where the size or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or are deliberately structured to avoid detection;

(iv) where a customer refuses to provide the information requested without reasonable explanation;

(v) where a customer who has newly entered into a business relationship uses the relationship for a single transaction or for only a very short period of time;

(vi) an extensive use of offshore accounts, companies or structures in circumstances where the customer's economic needs do not support such requirements;

(vii) unnecessary routing of funds through third party accounts;

(viii) the proffering of documents that appear fraudulent, unofficial, or are otherwise suspicious;

(ix) unusual transactions without an apparently profitable motive; or

(x) other circumstances as referred in national AML laws and regulations or as independently determined by the Relevant Person in accordance with its internal procedures.

(b) The requirement for employees to notify the Relevant Person's MLRO should include situations when no business relationship was developed because the circumstances were suspicious.

(c) A Relevant Person may allow its employees to consult with their line managers before sending a report to the MLRO. Such consultation does not prevent the making of a report whenever an employee has stated that he has knowledge, suspicion or reasonable grounds for knowing or suspecting that a person may be involved in money laundering. Whether or not an employee consults with his line manager or other employees, the responsibility remains with the employee to decide for himself/herself whether a notification to the MLRO should be made.

(d) An employee, including the MLRO, who considers that a person is engaged in or engaging in activity that he knows or suspects to be suspicious would not be expected to know the exact nature of the criminal offence or that the particular funds were definitely those arising from the crime of money laundering.

(e) CDD measures form the basis for recognising suspicious activity. Sufficient guidance must therefore be given to the Relevant Person's employees to enable them to form a suspicion or to recognise when they have reasonable grounds to suspect that money laundering is taking place. This should involve training that will enablerelevant employees to seek and assess the information that is required for them to judgewhether a person is involved in suspicious activity related to money laundering.

(f) A transaction that appears unusual is not necessarily suspicious. Even customers with a stable and predictable transaction profile may have occasional transactions that are unusual for them. Many customers will, for perfectly good reasons, have an erratic pattern of transactions or account activity. Unusual behaviour is, in the first instance, only a basis for further inquiry, which may in turn require judgement as to whether it is suspicious. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report then arises.

(g) Effective CDD measures may provide the basis for recognising unusual and suspicious activity. Where there is a customer relationship, suspicious activity will often be one that is inconsistent with a customer's known legitimate activity, or with the normal business activities for that type of account or customer. Therefore, the key to recognising 'suspicious activity' is knowing enough about the customer and the customer's normal expected activities to recognise when their activity is abnormal.

(h) A Relevant Person should implement policies and procedures whereby disciplinary action (including, but not limited to, a requirement of further training) is taken against an employee who fails to notify the Relevant Person's MLRO.

13.8. Responsibilities of Money Laundering Reporting Officer on receipt of a Suspicious Transaction Report

13.8.1. Activity upon notification

A Relevant Person must ensure that where the Relevant Person's MLRO receives a notification under AML 13.7.3., the MLRO, without delay:

(a) enquires into and documents the circumstances in relation to which the notification made under AML 13.7.3. was made;

(b) determines whether in accordance with the AML Law a STR must be made to the FIU and documents such determination; and

(c) if required, submits a STR to the FIU and promptly notifies the AFSA of such a submission.

13.8.2. Recording reasons for not making a Suspicious Transaction Report

Where, following a notification to the MLRO under AML 13.7.3, no STR is made, a Relevant Person must record the reasons for not making a STR.

13.8.3. Independence of Money Laundering Reporting Officer decision

(a) A Relevant Person must ensure that whether the MLRO decides to make or not to make a STR or TTR,his/her decision is made independently and is not subject to the consent or approval of any other person.

(b) Where a Relevant Person's MLRO has a suspicion of money laundering, and reasonably believes that performing the CDD process will tip-off the customer, he/she must not pursue the CDD process, and must submit a STR to the FIU.

Guidance on making Suspicious Transaction Reports

(a) In most cases, before deciding to make a report, the MLRO is likely to need access to the relevant business information. A Relevant Person must therefore take reasonable steps to give its MLRO access to such information. Relevant business information may include details of:

(i) the financial circumstances of a customer or beneficial owner, or any person on whose behalf the customer has been or is acting;

(ii) the features of the transactions, including, where appropriate, the jurisdiction in which the transaction took place; and

(iii) the underlying CDD information, and copies of the actual source documentation in respect of the customer.

(b) In addition, the MLRO may wish:

(i) to consider the level of identity information held on the customer, and any information on his personal circumstances that might be available to the firm; and

(ii) to review other transaction patterns and volumes through the account or accounts in the same name, the length of the business relationship and identification records held.

(c) Relevant Persons are reminded that the failure to report suspicions of money laundering may constitute a criminal offence.

(c-a) The AFSA may provide guidance and recommendations as it considers appropriate in assisting Relevant Persons in the detection and reporting of suspicious transactions to the FIU, in support of the FIU's objectives under the AML Law.

(d) STRs should be sent to the FIU in accordance with these Rules and AML Law. In the preparation of a STR, if a Relevant Person knows or assumes that the funds which form the subject of the report do not belong to a customerbut to a third party, this fact and the details of the Relevant Person's proposed course of further action in relation to the case should be included in the report.

(e) If a Relevant Person has reported a suspicion to the FIU, the FIU may instruct the Relevant Person on how to continue its business relationship, including effecting any transaction with a person. If the customer in question expresses his wish tomove the funds before the Relevant Person receives instruction from the FIU on how to proceed, the Relevant Person should immediately contact the FIU for further instructions.

Guidance on tipping-off

(a) Relevant Persons are reminded that in accordance with the AML Law, Relevant Persons or any of their employees must not tip-off any person, that is, inform any person that he/she is being scrutinised for possible involvement in suspicious activity related to money laundering, or that any other competent authority is investigating his/her possible involvement in suspicious activity relating to money laundering. In addition, the Relevant Persons must not disclose information contained in a STR or the fact that a STR may be or has been filed with the FIU or a suspicious transaction is being investigated.

(b) If a Relevant Person reasonably believes that conducting CDD measures will tip-off a customer or potential customer, it may choose not to pursue that process and should file a STR. Relevant Persons should ensure that their employees are aware of and sensitive to these issues when considering CDD measures.

Figure 1 – The Risk-Based Approach

14. GENERAL OBLIGATIONS

14.1. Training and Awareness

14.1.1. Training and Other Obligations

A Relevant Person must implement screening procedures to ensure high standards when hiring employees (Know Your Employee).

A Relevant Person must take appropriate measures to ensure that its employees:

(a) are made aware of the law relating to money laundering;

(b) are regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering;

(c) understand its policies, procedures, systems and controls related to money laundering and any changes to these;

(d) understand the types of activity that may constitute suspicious activity in the context of the business in which an employee is engaged and that may warrant a notification to the MLRO under AML 13.7.3.;

(e) understand its arrangements regarding the making of a notification to the MLRO under AML 13.7.3.;

(f) are aware of the prevailing techniques, methods and trends in money laundering relevant to the business of the Relevant Person;

(g) understand the risk of tipping-off and how to avoid informing a customer or potential customer that it is or may be the subject of a STR;

(h) understand the roles and responsibilities of employees in combating money laundering, including the identity and responsibility of the Relevant Person's MLRO and deputy, where applicable; and

(i) understand the relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions described in Chapter 13.

14.1.2. Appropriate measures

In determining what measures are appropriate under AML 14.1.1. Relevant Person must take account of:

(a) the nature of its business;

(b) its size; and

(c) the nature and extent of the risks of money laundering to which itsbusiness is subject.

The AFSA may impose additional training requirements in respect of all, or certain, relevant employees of a Relevant Person.

Guidance on training and awareness

(a) All relevant employees of a Relevant Person be given appropriate AML training as soon

Figure 1 – The Risk-Based Approach

as reasonably practicable after commencing employment with the Relevant Person. A relevant employee means a member of the senior management or operational staff, any employee with customer contact, or any employee who handles (or may handle) customer monies or assets, and any other employee who might encounter money laundering in the business.

(b) Relevant Persons should take a RBA to AML training. AML training should be provided by a Relevant Person to each of its relevant employees at intervals appropriate to the role and responsibilities of the employee. In the case of an Authorised Firm, training should be provided to each relevant employee at least annually.

(c) AML training provided by a Relevant Person need not be in a formal classroom setting, rather it may be via an online course or any other similarly formal and documented manner.

14.2. Groups, branches and subsidiaries

14.2.1. Application of policies to Group entities

A Relevant Person which is a Centre Participant (excluding recognised or registered entities that are branches) must ensure that its policies, procedures,systems and controls required by AML 4.1.1. apply to:

(a) all of its branches or Subsidiaries established in a jurisdiction other than the AIFC; and

(b) all of its Group entities that are Centre Participants.

14.2.2. Equality of other jurisdictions

The requirement in AML 14.2.1. does not apply if the Relevant Person can satisfy the AFSA that the relevant branch, Subsidiary or Group entity is subject to regulation, including AML, by a Financial Services Regulator or other competent authority in a country with AML regulations which are equivalent to the standards set out in the FATF Recommendations and is supervised for compliance with such regulations.

Where the law of another jurisdiction does not permit the implementation of policies, procedures, systems and controls consistent with those of the Relevant Person, the Relevant Person must:

(a) inform the AFSA in writing; and

(b) apply appropriate additional measures to manage the money laundering risks posed by the relevant branch or Subsidiary.

14.2.3. Communication and documentation

In relation to the Group entities referred to in AML 14.2.1., a Relevant Person must:

(a) communicate the policies and procedures (and RBA where relevant) which it establishes and maintains in accordance with these Rules to its Group entities, branches and Subsidiaries; and

(b) document the basis for its satisfaction that the requirement in AML 14.1.1.(b) is met.

14.2.4. Enforcement

In relation to an Authorised Firm, if the AFSA is not satisfied in respect of AML compliance of its branches and Subsidiaries in a particular jurisdiction, it may take action, including making it a condition on the Authorised Firm's Licence that it must not operate a branch or Subsidiary in

Figure 1 – The Risk-Based Approach

that jurisdiction.

14.3. Group policies

14.3.1. Group policy compliance

A Relevant Person which is part of a Group must ensure that it:

(a) includes the provisions in policies and procedures of the Group concerning information sharing between Group entities on the Group's compliance, audit and AML functions. The information that is being shared should include CDD information that had been reviewed for money laundering risk mitigation purposes and analysis (if any) of transactions or activities which appear unusual;

(a-a) understands the policies and procedures covering the sharing of information between Group entities, particularly when sharing CDD information;

(b) has in place adequate safeguards on the prevention of tipping-off and the confidentiality and use of information exchanged between Group entities;

(c) remains aware of the money laundering risks of the Group as a whole and of its exposure to the Group and takes active steps to mitigate such risks;

(d) contributes to a Group-wide risk assessment to identify and assess money laundering risks for the Group;

(e) provides its Group-wide compliance, audit and AML functions with customer account and transaction information from branches and subsidiaries for AML purposes; and

(f) ensures that its branches and majority-owned subsidiaries in host countries implement the requirements of the AIFC, to the extent that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering risks, and inform the AFSA of such measures.

14.4. Notifications

14.4.1. Notification obligation

A Relevant Person must inform the AFSA in writing quarterly about number, reasons, and outcomes if, in relation to itsactivities carried on as part of the AIFC or in relation to any of its branches or Subsidiaries, it:

(a) receives an ad-hoc (specific) request for providing detailed information as regards particular customer or transaction from a regulator or agency responsible for AML, CFT, or sanctions compliance in relation to potential money laundering or sanctions contravention[4];

(b) becomes aware, or has reasonable grounds to believe, that a money laundering event has occurred or may have occurred in or through its business;

(c) becomes aware of any money laundering or sanctions matter in relation to the Relevant Person or a member of its Group which could result in adverse reputational consequences to the Relevant Person; or

[4] Does not apply to the regular interaction between a reporting entity and FIU as regards technical issues related to filling out of F1.

Figure 1 – The Risk-Based Approach

(d) becomes aware of a significant contravention of these Rules or a contravention of the relevant Kazakhstan legislation by the Relevant Person or any of its employees.

14.5. Record keeping

14.5.1. Obligation to keep records

A Relevant Person must maintain the following records:

(a) a copy of all documents and information obtained in conducting initial and on-going CDD;

(b) the supporting records (consisting of the original documents or certified copies) in respect of the customer business relationship, including transactions;

(c) notifications made under AML 13.7.3.;

(d) STRs and any relevant supporting documents and information, including internal findings and analysis;

(e) any relevant communications with the FIU; and

(f) the documents in AML 14.5.2.,

for at least six years from the date on which the notification or report was made, the business relationship ends or the transaction is completed, whichever occurs last.

14.5.2. Documentation obligation

A Relevant Person must document, and provide to the AFSA on request, any of thefollowing:

(a) the risk assessments of its business undertaken under AML 4.1.1.;

(b) how the assessments in (a) were used for the purposes of complying with AML 5.1.1.(a);

(c) the risk assessments of the customer undertaken under AML 5.1.1.; and

(d) the determinations made under AML 5.1.1.

14.5.3. Location of Records

Where the records referred to in AML 14.5.1. are kept by the Relevant Person in the care of an entity that is not a Centre Participant, a Relevant Person must:

(a) take reasonable steps to ensure that the records are held in a manner consistent with these Rules;

(b) ensure that the records are easily accessible to the Relevant Person; and

(c) upon request by the AFSA, ensure that the records are available for inspection within a reasonable period.

14.5.4. Data protection legislation

A Relevant Person must:

(a) verify if there is secrecy or data protection legislation that would restrict access without delay to the records referred to in AML 14.5.1. by the Relevant Person, the AFSA, or

Figure 1 – The Risk-Based Approach

applicable Kazakhstan law; and

(b) where such legislation exists, obtain without delay certified copies of the relevant records and keep such copies in a jurisdiction which allows access by those persons identified in (a).

14.5.5. Training records

A Relevant Person must be able to demonstrate that it has complied with the training and awareness requirements in Chapter 14 through appropriate measures, including the maintenance of relevant training records.

Guidance on record keeping

(a) The records required to be kept under AML 14.5. may be kept in electronic format, if such records are readily accessible and available to respond promptly to any AFSA requests for information. Authorised Persons are reminded of their obligations in GEN 5.9.

(b) If the date on which the business relationship with a customer has ended remains unclear, it may be taken to have ended on the date of the completion of the last transaction.

(c) The records maintained by a Relevant Person should be kept in such a manner that:

(i) the AFSA, or another competent authority are able to assess the RelevantPerson's compliance with legislation applicable in the AIFC;

(ii) any transaction which was processed by or through the Relevant Person on behalf of a customer or other third party can be reconstructed;

(iii) any customer or third party can be identified; and

(iv) the Relevant Person can satisfy any regulatory enquiryor court order to disclose information within the time indicated in such enquiry or court order.

(d) In complying with AML 14.5.3., Authorised Persons are reminded of their obligations in GEN 5.9.

(e) "Appropriate measures" in AML 14.5.5. may include the maintenance of a training log setting out details of:

(i) the dates when the training was given;

(ii) the nature of the training; and

(iii) the names of employees who received the training.

14.6. Audit

14.6.1. Audit obligation

An Authorised Person must ensure that its audit function, established under GEN 5.5.1. includes regular reviews and assessments (not less than once in two years) of the effectiveness of the Authorised Person's AML policies,procedures, systems and controls, and its compliance with its obligations in these Rules.

Guidance on audit

Figure 1 – The Risk-Based Approach

(a) The review and assessment undertaken for the purposes of AML 14.6.1. may be undertaken:

(i) internally by the Authorised Person's internal audit function; or

(ii) by a competent firm of independent auditors or compliance professionals.

(b) The review and assessment undertaken for the purposes of AML 14.6.1. should cover at least the following:

(i) sample testing of compliance with the Authorised Person's CDD arrangements;
(ii) the adequacy of the Authorised Person's AML/CFT Systems, ML/TF risk assessment framework and application of risk-based approach;
(iii) the effectiveness of the system for recognising and reporting suspicious transactions;

(iv) an analysis of all notifications made to the MLRO to highlight any area where procedures or training may need to be enhanced;

(v) a review of the nature and frequency of the dialogue between the senior management and the MLRO; and

(vi) the level of awareness of staff having AML/CFT responsibilities.

14.7. Communication with the Regulator

14.7.1. Communication obligation

A Relevant Person must:

(a) be open and cooperative in all its dealings with the Regulator; and

(b) ensure that any communication with the Regulator is conducted in the English language.

14.8. Protection for Disclosures

14.8.1. Protection

A Relevant Person must ensure that it does not prejudice a person who discloses any information on behalf of the Relevant Person regarding money laundering to the AFSA or to any other relevant body involved in the prevention of money laundering.

A Relevant Person and a person, who submits a STR on behalf of the Relevant Person, are not subject to any civil liability or criminal prosecution under the Kazakhstan law resulting from the submission of the STR, even if they did not know precisely what the criminal activity was, and regardless of whether illegal activity actually occurred.

Guidance on Protection for Disclosures

A "relevant body" in AML 14.8.1. would include the FIU.

Annex 1

List of Defined Terms for AML Rules and associated guidelines and requirements

Definition	Interpretation
AML	for the purposes of these Rules means anti-money laundering
AML Rules	for the purposes of these Rules means AIFC Anti-Money Laundering, Counter – Terrorist Financing

Figure 1 – The Risk-Based Approach

	and Sanctions Rules
AML Law	Law of the Republic of Kazakhstan No 191-IV dated 28 August 2009 on counteracting legalisation (laundering) of proceeds obtained through criminal means and financing of terrorism
AIFC acts	AIFC acts adopted by the relevant decision-making body (Regulations, Rules, Guidance, etc.)
BURA	Business Risk Assessment
CFT	countering the financing of terrorism
CRA	Customer Risk Assessment
Criminal Code	Criminal Code of the Republic of Kazakhstan No 226-V dated 3 July 2014
geographic area (state or territory) considered to be an area of high risk	Geographic areas considered to be an area of high risk include: • countries or jurisdictions that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies; • countries or jurisdictions subject to sanctions, embargos or similar measures issued by UN, US, EU, UK; • countries or jurisdictions which are more vulnerable to corruption; • countries or jurisdictions that are believed to have strong links to terrorist activities. • countries known as tax heavens (offshore jurisdictions)
KYC	Know Your Customer, adequate customer identification procedures
KYE	Know Your Employee, adequate screening procedures to ensure high standards when hiring employees
money laundering	a reference to 'money laundering' also includes a reference to terrorist financing and financing the proliferation of weapons of mass destruction
sanctions violation	an action aimed the violation evasion or circumvention of EU, US, UK sanctions, such as but not limited to: • establishing relations with prohibited persons or entities, • breaching stipulated embargoes, • providing prohibited or restricted economic and financial services, • transferring, receiving funds or providing false information to conceal operations or funds that should be restricted or prohibited. • avoiding or circumventing sanctions
sanctions list	a list of all individuals, groups, and other entities sanctioned by the United Nations and FIU. This includes asset freezes, travel bans, and arms embargoes.
senior management	a high-level executive who oversees the operations and performance of one or more departments within a company
SOF	Source(s) of funds
SOW	Source(s) of wealth
tipping-off	to warn someone secretly about something that will happen, so that they can take action or prevent it from happening
TTR	Threshold Transaction Report
Transparency International	global civil society organisation leading the fight against corruption
UNSC	United Nations Security Council
watchlists	a set (database, register, list) of information on individuals, organisations, and countries that deserve special attention and

	appropriate actions, including lists of unilateral sanctions by jurisdictions or authorities (target, sanction, embargo)
Wolfsberg Group	an association of 12 global banks which aims to develop frameworks and guidance for the management of financial crime risks

Figure 1 – The Risk-Based Approach

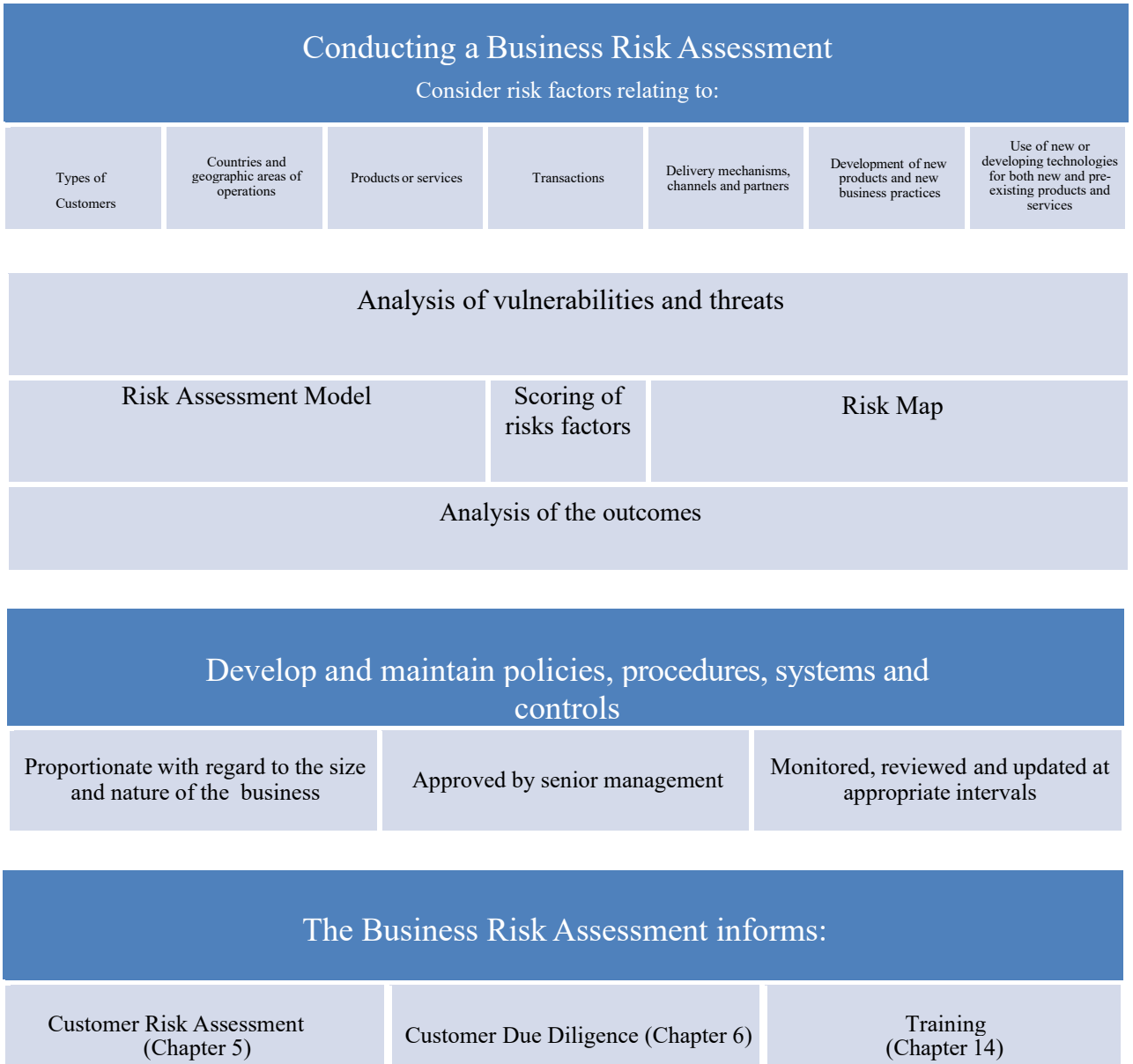

Figure 2 – Customer Risk Assessment