Draft

In this Draft, a blue font and underlining indicates new text

---

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

(AML)

Astana International Financial Centre, Astana

Contents

1. INTRODUCTION

1.1. Overview of the AML Rules

(a) The Anti-Money Laundering ("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.

1.2. Purpose of 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 AML, counter-terrorist financing ("CTF"), and sanctions compliance. This means that they apply to Authorised Firms, Authorised Market Institutions, Designated Non- Financial Businesses and Professions ("DNFBPs"), 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 Resolutions ("UNSCRs") and unilateral sanctions imposed by other jurisdictions which may apply to a Relevant Persons depending on the Relevant Person's jurisdiction of origin, its business and/or customer base.

1.3. Money Laundering and Terrorist Financing

(a) Money laundering takes many forms, including:

(i) acquiring, possessing, or using the proceeds of crime;

(ii) concealing, disguising, converting, or transferring the proceeds of crime; and

(iii) entering into arrangements to facilitate the acquisition, retention,

use, or control of criminal property by or on behalf of another person.

(b) The techniques used by money launderers constantly evolve to match the source and amount of funds to be laundered, and the legislative, regulatory and law enforcement environment of the market in which the money launderer wishes to operate.

(c) Terrorist financing is the collection and provision of funds with the intention that they may be used to support terrorist acts or organisations. There can be similarities between the movement of terrorist property and the laundering of criminal property: some terrorist groups are known to have well established links with organised criminal activity. Terrorist organisations often control property and funds from a variety of sources and employ sophisticated techniques to manage these funds, and to move them between jurisdictions.

1.4. Financial Action Task Force

(a) The Financial Action Task Force ("FATF") is an inter-governmental body whose purpose is the development and promotion of international standards to combat money laundering and terrorist financing.

(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 and terrorist financing methods. These can be found on the FATF website www.fatf-gafi.org. Some international groupings, official or informal, publish material that may be useful as context and background in informing the approach adopted by Relevant Persons to AML and CTF. These groupings include Transparency International (www.transparency.org.uk) and the Wolfsberg Group (www.wolfsberg-principles.com).

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

sanctions and resolutions (See Chapter 12).

(e) The FATF has issued guidance on a number of specific UNSC sanctions and resolutions 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 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 positive steps 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.

(d) Chapter 5 explains the concept of customer risk assessments.

(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 Chapter 11 sets out obligations relating to wire transfers.

(h) Chapter 12 sets out a Relevant Person's obligations in relation to UNSCRs, sanctions, and government, regulatory and international findings in relation to AML, CTF, 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 Suspicious Activity Reports ("SARs") which 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 used in these Rules are set out in the Astana International Financial Centre Glossary.

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; 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; or

(iv) a Registered Auditor.

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 the decision-making processes and must take ownership of the risk-based approach 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 taking enforcement action against any person including any one or more of the following persons in respect of a breach 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.

3. GUIDANCE ON KAZAKHSTAN CRIMINAL LAW

3.1. Kazakhstan criminal law

(a) Kazakhstan's criminal legislation, including the Criminal Code, 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 legislation 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 and terrorist financing to which its business is exposed, and must establish and maintain policies, controls and procedures to mitigate and manage the risks 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 conduct business and customer risk assessment

In order to identify and assess the risks of money laundering and terrorist financing 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 and terrorist financing 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 be identified and assessed by a Relevant Person prior to the launch or use of such products, practices and technologies.

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, controls and procedures adequately mitigate the risks identified;

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

(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, controls and procedures

4.3.1. Requirements of policies, controls and procedures

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

(a) proportionate to the nature, scale and complexity 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, risk management, customer identification, transaction monitoring and studying, employees training and awareness programs;

(c) approved by its senior management; and

(d) monitored, reviewed and updated regularly.

4.3.2. Purpose of policies, controls and procedures

The policies, controls and procedures must provide for the identification and scrutiny of:

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

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

(c) other activity which the Relevant Person regards as particularly likely by its nature to be related to money laundering or terrorist financing.

4.3.3. Record of policies, controls and procedures

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

Guidance on the risk based approach

(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 below. 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 effective way.

(b) No system of checks will detect and prevent all money laundering or terrorist financing. A 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 or terrorist financing. 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) Unless a Relevant Person understands the money laundering risks to which it is exposed, it cannot take appropriate steps to prevent its business being used for the purposes of money laundering. Money laundering risks vary from business to business depending on the nature of the business, the type of customers a business has, and the nature of the products and services sold.

(f) 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.

(g) Using the RBA, a Relevant Person must assess its own vulnerabilities to money laundering and take 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).

(h) Risk management is a continuous process, carried out on a dynamic basis. A money laundering and terrorist financing risk assessment is not a one-time exercise. Relevant Persons must ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review and that any changes made to policies, controls and procedures are recorded.

5. CUSTOMER RISK ASSESSMENT

5.1. Assessing customer ML risks

5.1.1. Requirement to conduct a customer risk assessment

A Relevant Person must:

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

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

5.1.2. Timing of the customer risk assessment

The customer risk assessment in AML 5.1.1 must be completed prior to undertaking Customer Due Diligence 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 beneficiary of a life insurance policy, where applicable; and

(h) consider the outputs of the business risk assessment under Chapter 5.

5.1.4. Identification of Politically Exposed Persons

The policies, controls and procedures 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 arrangements

A Relevant Person must not establish a business relationship with a customer which is a legal person if the ownership or control arrangements 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 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.

(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 below, requires a Relevant Person to allocate an appropriate risk rating to every customer. Risk ratings are to be described as "low", "medium" or "high", on a sliding numeric scale with 1 to 3 as "low" risk, 4 to 7 as "medium" risk, and 8 to 10 as "high" risk. Depending on the outcome of 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 undertaken.

(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 person would not normally be a customer of a Relevant Person merely because such person receives marketing information from a Relevant Person or where a Relevant Person refers a person who is not a customer to a third party (including a Group member).

(c) A counterparty would generally be a "customer" for the purposes of these Rules and would therefore require a Relevant Person to undertake 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 the following customer risk factors which may indicate that a customer poses a higher risk of money laundering:

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

(ii) the customer is resident in a geographical area considered by 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; and

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

(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 terrorist financing; and

(ii) countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations Security Council 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 for terrorism.

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;

(ii) an individual resident in a geographical area of lower risk which has AML 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 risk assessment(s) it has undertaken in accordance with Chapter 4.

Guidance on Shell Banks

(a) AML 5.1.6 prohibits a Relevant Person from establishing or maintaining a business relationship with a Shell Bank.

(b) The presence of a local agent or administrative staff would not constitute a physical presence in the country in which the customer is incorporated or licensed.

6. CUSTOMER DUE DILIGENCE

6.1. Undertaking Customer Due Diligence

6.1.1. Obligation to undertake Customer Due Diligence

A Relevant Person must:

(a) undertake CDD under AML 6.3.1 for each of its customers; and

(b) in addition to (a), undertake EDD under AML 7.1.1 in respect of any customer it has assigned as high risk.

6.1.2. Undertaking Simplified Due Diligence

A Relevant Person may undertake 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. Simplified measures should not be conducted whenever there is a suspicion of money laundering and/or terrorist financing.

Guidance on Customer Due Diligence

(a) A Relevant Person should undertake CDD in a manner proportionate to the customer's money laundering risks identified under Chapter 6.

(b) 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 undertaken under AML 7.1.1. For low risk customers, AML 6.3.1 may be modified based on risk in accordance with AML 8.1.1.

(c) 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. 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.

6.2. Timing of Customer Due Diligence

6.2.1. Establishment of business relationship

A Relevant Person must apply 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 undertake appropriate Customer Due Diligence 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 Customer Due Diligence;

(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 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 relationship;

(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 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 AML 6.2.3(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.

(b) In AML 6.2.3, 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 customer to 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 SARs and tipping off.

(d) For the purposes of AML 6.2.3(d), in most situations "as soon as reasonably practicable" would be within 30 days after the establishment of a business relationship.

6.3. Undertaking Customer Due Diligence

6.3.1. Verification of obligations

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

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

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

(c) understand the customer's sources of funds;

(d) understand the customer's sources of wealth; and

(e) undertake 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 any named beneficiaries of the insurance policy;

(b) 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 of the insurance policy;

(c) 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; and

(d) 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 suspicious transaction report.

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 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.

Guidance on undertaking 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 who holds the position of senior managing official; 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 higher risk situations, identification information is to be independently verified, using both public and non-public sources.

(f) In complying with AML 6.3.1(b) 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 (e.g. a specific bank or trading account held with a specific financial institution) and whether that funding is consistent with the customer's source of wealth. 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, customer questionnaire or a memo of a call with the relationship manager at a financial institution.

(g) In complying with AML 6.3.1(c) a Relevant Person is required to "understand" a customer's source of wealth. For a natural person, this might include questions about the source of wealth in an application form or customer questionnaire. The understanding may also be gained through interactions with the relationship manager at a financial

institution. It could also be gained by obtaining information from a reliable and independent publicly available source, for example, from published accounts or a reputable news source. The understanding need not be a dollar for dollar account of the customer's global wealth, 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 should be clearly documented.

(h) Understanding a customer's sources of funds and wealth is also important for the purposes of undertaking on-going due diligence under AML 6.3.1(d) 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.

(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.

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. There are no explicit ownership or control thresholds in defining the beneficial owner because the applicable threshold to adopt will ultimately depend on the risks associated with the customer, and so a Relevant Person must adopt the RBA and pursue on reasonable grounds an approach which is proportionate to the risks identified. A Relevant Person should not set fixed thresholds for identifying the beneficial owner without objective and documented justification. An overly formal approach to defining the beneficial owner may result in a criminal "gaming" the system by always keeping his financial interest below the relevant threshold.

(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, this 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.

(g) Where no natural person is identified as a beneficial owner, the relevant natural person who holds the position of senior managing official 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 associates. PEP status itself does not incriminate individuals or entities. It does, however, put the customer into a higher risk category.

(b) Generally, a foreign 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 undertaking on-going CDD under AML 6.3.1, a Relevant Person must, using the risk- based approach:

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

(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 (b);

(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; and

(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.

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 undertaken 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 sanctions lists

6.5.1. Sanctions list review

A Relevant Person must review its customers, their business and transactions against United Nations Security Council sanctions lists and against any other Kazakhstan Sanctions List when complying with AML 6.4.1(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 or suspend any existing business relationship with the customer;

(e) return any monies or assets received from the customer; and

(f) consider whether the inability to conduct or complete Customer Due Diligence necessitates the making of a Suspicious Activity Report (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 breach of the AML Law; or

(b) the Committee on Financial Monitoring of the Ministry of Finance (the "Committee") 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. However, for existing customers, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances. Whichever route is taken; 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

Where a Relevant Person is required to undertake 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 sources of funds;

(ii) the customer's sources of wealth;

(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 business and 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 and wealth because the source of the funds would normally be the beneficial owner and not the 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 transaction which 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 its financial 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 undertake 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 source of funds or source of wealth;

(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 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 undertaken 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 the extent that this is commercially necessary. On the other hand, a low risk customer which is undertaking a complex transaction might require more comprehensive SDD.

(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 Customer Due Diligence on its behalf:

(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 from the third party in AML 9.1.1;

(b) it takes adequate steps to satisfy itself that certified copies of the documents used to undertake the relevant elements of Customer Due Diligence will be available from the third party on request without delay;

(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 FATF; and

(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.

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.

Guidance on reliance

(a) In complying with AML 9.1.3(a) "immediately obtaining the necessary CDD information" means obtaining all relevant CDD information, beyond merely basic information such as the name and address of the customer or beneficial owner. The relevant information could be sent by email or other appropriate means.

(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. Compliance can be achieved by having that

relevant information sent by fax or email. For the avoidance of doubt, a Relevant Person is not required automatically to obtain the underlying certified documents used by the third party to undertake 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 undertaken; and

(ii) to undertake 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 undertake 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 a foreign jurisdiction to conduct one or more elements of CDD on its behalf, the Relevant Person must ensure that the foreign jurisdiction has AML regulations that are the reasonable equivalent of the standards in the FATF Recommendations (see AML 9.1.3(c)).

(g) When assessing if AML regulations in another jurisdiction are equivalent to 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 specialised 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 undertake appropriate due diligence to assure itself of the suitability of the outsourced service provider and should ensure that the outsourced service provider's obligations are clearly documented in a binding agreement.

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) undertake 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 or terrorist financing 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) ensure that the respective responsibilities of the parties to the correspondent banking relationship are properly documented; and

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

(ii) will conduct ongoing monitoring for its customers; 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, particularly to satisfy the requirement in (c) above, 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/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 it is regulated and supervised (at least for AML and CFT purposes) by a regulatory or governmental authority, body or agency equivalent to the Regulator in each jurisdiction in which it operates;

(iv) whether each foreign jurisdiction in which it operates has an effective AML/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 on a regular basis.

An Authorised Firm must:

(i) not enter into, or continue a correspondent banking relationship with a Shell Bank;

and

(j) 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 to be 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. Shell Banks

10.3.2 Prohibition on 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 customer due diligence measures for all of its customers and verified their identity; and

(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 suspicious transaction report to the FIU.

10.5. Payment processing using On-line services

10.5.1 Electronic verification of identification documentation

(a) An Authorised Firm may rely on electronic verification of identification documentation if it complies with the risk-based approach and other requirements of these rules.

(b) An Authorised Firm must make and keep a record that clearly demonstrates the basis on which it relied 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:

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

(ii) the same risk-based methodology.

10.5.2 Concession for certain non-face to face transactions

(a) This rule applies if:

(i) a customer of an Authorised Firm would normally be required to produce evidence of identity before transacting business with the Authorised Firm involving the making of a payment; and

(ii) it is reasonable in all the circumstances for payment to be made by post or electronically, or for details of the payment to be given by telephone; and

(iii) payment is to be made from an account held in the customer's name at a financial institution.

(b) However, this rule does not apply if:

(iv) initial or future payments can be received from third parties; or

(v) cash withdrawals can be made, unless the withdrawals can only be made by the customer on a face-to-face basis where identity can be confirmed; or

(vi) redemption or withdrawal proceeds can be paid to a third party or to an account that cannot be confirmed as belonging to the customer, unless the proceeds can only be paid to an executor or personal representative on the death of the customer.

(c) If this rule applies, the firm may waive identification requirements for the

customer. However, a repayment may be made to another firm only if the other firm has confirmed that the amount of the repayment is either to be paid to the customer or reinvested elsewhere in the name of the customer.

(d) This rule applies to a joint account as if a reference to the customer included a reference to any of the customers.

11. WIRE TRANSFERS

11.1. Definitions

11.1.1. Defined terms

In this section:

(a) "beneficiary" means the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.

(b) "originator" means the account holder who instructs the wire transfer from the relevant account, or where there is no account, the natural or legal person that places the order with the ordering Financial institution to perform the wire transfer; and

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

11.2. Wire transfer requirements

11.2.1. Obligations in respect of wire transfer

An Authorised Person must:

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

(e) monitor wire transfers for the purpose of detecting those wire transfers that do not contain originator and beneficiary information and take appropriate measures to identify any money laundering risks.

11.2.2. Financial Institutions acting on their own behalf

The requirement in AML 11.2.1 does not apply to an Authorised Person who transfers funds to another Financial Institution where both the originator and the beneficiary are Financial Institutions acting on their own behalf.

11.2.3. Wire transfer requirements

An Authorised Person must ensure that information accompanying all wire transfers contains at a minimum:

(a) the name of the originator:

(b) the originator account number where such an account is used to process the transaction;

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

(d) the name of the beneficiary; and

(e) the beneficiary account number where such an account is used to process the transaction.

Guidance on wire transfers

(a) In the absence of an account number, a unique transaction reference number should be included which permits traceability of the transaction.

(b) Concealing or removing in a wire transfer any of the information required by AML 11.2.1 would be a breach of the requirement to ensure that the wire transfer contains accurate originator and beneficiary information.

12. SANCTIONS

12.1. Relevant United Nations 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 United Nations Security Council or by the Republic of Kazakhstan. 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 United Nations Security Council or by the Republic of Kazakhstan.

12.1.2. Notification obligation

A Relevant Person must report to the Committee on financial monitoring of the Ministry of Finance of the Republic of Kazakhstan any assets frozen or actions taken in compliance with the prohibition requirements of the relevant resolutions or sanctions issued by the United Nations Security Council or by the Republic of Kazakhstan, including attempted transactions.

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

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

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

(h) 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 United Nations Security Council.

12.1.3. Notification requirements

A Relevant Person must ensure that the notification stipulated in AML 12.1.2 above includes the following 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 or that it may need to undertake 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, terrorist financing or the financing of weapons of mass destruction 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, terrorist financing or the financing of weapons of mass destruction.

(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 article 13 of the Kazakhstan AML law in relation to freezing assets and blocking transactions and must also consider whether it is necessary to file a suspicious activity report.

(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 terrorist financing or financing of weapons of mass destruction.

(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 issued by the United Nations Security Council 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:

(i) the government of the Republic of Kazakhstan;

(j) the National Bank of Kazakhstan;

(k) Kazakhstan state agencies;

(l) the AFSA; and

(m) 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, terrorist financing or the financing of weapons of mass destruction 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 or terrorist financing or the financing of weapons of mass destruction 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.

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/CTF 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 14 on Suspicious Activity Reports.

(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 United Nations Security Council, 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 Kazakhstan Ministry of Finance, European Union, the United Kingdom (HM Treasury) lists, and the United States of 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 undertake 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, 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 is a Director, Partner, Principal Representative, or Senior Manager of an Authorised Person and who has responsibility for the implementation and oversight of an Authorised Person's AML policies, procedures, systems and controls.

13.1.2. Appointment of MLRO

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.

13.1.3. Residency Requirement

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

Guidance on appointment of MLRO

(a) Under GEN 2.1.2, the MLRO function is a mandatory appointment. For the avoidance of doubt, the individual appointed as the MLRO of an Authorised Firm, other than a Representative Office, is the same individual who holds the Designated Function of MLRO of that Authorised Firm.

(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. Deputy Money Laundering Reporting Officer

13.2.1. Appointment of deputy

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.

13.3. 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

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 an MLRO

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 to act on his own authority and to act independently in carrying out his responsibility;

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

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

Guidance on qualities of an MLRO

A Relevant Person will need to consider this AML 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 a MLRO

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) making SARs in accordance with applicable Kazakhstan law;

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

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

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

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

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 four 4 months of its financial year end.

13.7.1. Defined terms

In this part, "money laundering" and "terrorist financing" mean the criminal offences defined in the AML Law.

13.7.2. Threshold Transactions Controls

A Relevant Person must establish and maintain procedures, systems and controls to monitor, detect and report transactions above defined thresholds in accordance with the AML Law.

13.7.3. Suspicious Activity 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 or terrorist financing.

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

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

13.7.5. Employee reporting to MLRO

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 or terrorist financing, that employee promptly notifies the Relevant Person's MLRO and provides the MLRO with all relevant information within the employee's knowledge.

Guidance on Suspicious Activity 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; or

(ix) unusual transactions without an apparently profitable motive.

(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 or terrorist financing.

(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 or terrorist financing is taking place. This should involve training that will

enable relevant employees to seek and assess the information that is required for them to judge whether a person is involved in suspicious activity related to money laundering or terrorist financing.

(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 MLRO on receipt of a Suspicious Activity 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 Kazakhstan criminal legislation a SAR must be made to the Committee and documents such determination; and

(c) if required, submits a SAR to the Committee.

13.8.2. Recording reasons for not making a Suspicious Activity Report

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

13.8.3. Independence of MLRO decision

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

Guidance on making Suspicious Activity 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 or terrorist financing may constitute a criminal offence.

(d) SARs should be sent to the Committee in the way prescribed by Decree 1484 of the Government of Kazakhstan. In the preparation of a SAR, if a Relevant Person knows or assumes that the funds which form the subject of the report do not belong to a customer but 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 Committee, the Committee 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 to move the funds before the Relevant Person receives instruction from the Committee on

how to proceed, the Relevant Person should immediately contact the Committee 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.

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

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.

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

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

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

(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;

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

(b) 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 SAR;

(c) 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

(d) 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 and terrorist financing to which its business 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 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 risk-based approach 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 must ensure that its policies, procedures, systems and controls required by AML 4.1.1 apply to:

(a) all of its branches or Subsidiaries; 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

A Relevant Person must:

(a) communicate the policies and procedures 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 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) understands the policies and procedures covering the sharing of

information between Group entities, particularly when sharing Customer Due Diligence information;

(b) has in place adequate safeguards on the confidentiality and use of information exchanged between Group entities, including satisfying relevant data protection legislation;

(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; and

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

14.4. Notifications

14.4.1. Notification obligation

A Relevant Person must inform the AFSA in writing as soon as possible if, in relation to its activities carried on as part of the AIFC or in relation to any of its branches or Subsidiaries, it:

(a) receives a request for information from a regulator or agency responsible for AML, counter-terrorism financing, or sanctions compliance in connection with potential money laundering, terrorist financing, or sanctions breaches;

(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

(d) becomes aware of a significant breach of a AML in these Rules or a breach 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 undertaking initial and on- going Customer Due Diligence;

(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) Suspicious Activity Reports and any relevant supporting documents and information, including internal findings and analysis;

(e) any relevant communications with the Committee; 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 AIFC or the AFSA on request, any of the following:

(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 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 AIFC 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 AIFC, the AFSA, or another competent authority are able to assess the Relevant
Person's compliance with legislation applicable to 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, within an appropriate time, any regulatory enquiry or court order to disclose information.

(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 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

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

(iii) a review of the nature and frequency of the dialogue between the senior management and the MLRO.

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. Employee Disclosures

14.8.1. Employee protection

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

Guidance on Employee Disclosures

(a) A "relevant body" in AML 14.8.1 would include the Committee.

Figure 1 – The Risk Based Approach

Figure 2 – Customer Risk Assessment