Decision No. E/81/2021

Instructions to Insurance and Takaful Companies, Brokers and Agents on the Implementation of the Provisions of the Law on Combating Money Laundering and Terrorism Financing.

Based on the Insurance Companies Law enacted by Royal Decree No. 12/79; and
Takaful Insurance Law No. 11/2016; and
Money Laundering and Terrorism Financing Law enacted by Royal Decree No. 30/2016; and
The Regulation for the Insurance Companies issued by Ministerial Decision No. 5/80; and
Takaful Regulation No. 103/2019; and
Decision No. E/72/2019 on the Instructions to the Insurance Companies, Brokers and Agents on the Implementation of the Law on Combating Money Laundering and Terrorism Financing No. E/3/2020;
In the interest of the public

It has been decided

First Article

The attached instructions to insurance and Takaful companies, brokers and agents shall have effect as regards the implementation of the provisions of the Law on Combating Money Laundering and Terrorism Financing.

Second Article

Decision No. E/3/2020 shall be repealed as well as anything infringing this decision and the attached instructions or is inconsistent with their provisions.

Third Article

All concerned entities shall enforce this decision as from the date of issuance.

Abdullah Salim Abdullah Al Salmi
Executive President
Issued on: Dhul Qaida 26, 1442 H
Corresponding to: July 7, 2021

Instructions to the Insurance and Takaful Companies, Brokers and Agents on the Implementation of the Provisions of the Law on Combating Money Laundering and Terrorism Financing

Chapter 1

Definitions and General Provisions

Article 1

In the application of these instructions words and expressions shall have the same meaning in the Law on Combating Money Laundering and Financing Terrorism, and the following words and expressions shall have the meaning respectively ascribed to them unless the context otherwise requires.

Law: Law on Combating Money Laundering and Terrorism Financing enacted by Royal Decree No. 30/2016

Centre: National Centre for Financial Information

CMA: Capital Market Authority

Committee: National Committee for Combating Money Laundering and Terrorism Financing

Licensed entities: Insurance and Takaful companies, insurance broker and agents.

Third party: a financial institution or designated non-financial business or profession in the Sultanate of Oman or a foreign country that is regulated and supervised by a competent authority to ensure compliance with AML/CFT requirements and is subject to AML/CFT requirements equivalent to those established in Oman, especially in relation to the Customer Due Diligence and record keeping.

Article 2

The purpose of these instructions is to provide direction to licensed entities to assist them to comply with their obligations under Article (51) (c) of the Law.

Chapter 2

Article 3

1. Licensed entities must assess and understand the money laundering and terrorism financing risks inherent to their business. , the risk assessment, and any underlying information must be documented in writing, be kept up-to-date and be readily available for the CMA or any other competent authority for review, on request. In assessing money laundering and terrorism financing risks, licensed entities must give consideration at least to the following factors:

    a) Risk related to customer,;
    b) Risk related to countries or geographic area in which the customer and/or is domiciled, in which the customer operates and/or the place of origination or destination of a transaction;
    c) Risk related to countries or geographic areas in which the licensed entity maintains operations and/or conducts business (target markets);
    d) Risk related to the nature, diversity and complexity of its products, services and transactions offered; and
    e) Delivery channel risks for products and services, in particular the extent to which the licensed entity deals directly with the customer and the extent to which it relies on third parties to conduct customer due diligence or other obligations and in particular, the number of intermediaries or distributors involved.

2. Licensed entities must take into account any variables or combination of variables, which may increase or decrease the money laundering or terrorism financing risk in a specific situation. Such variables include:
        a) The purpose of an account, policy, transaction or business relationship;
        b) The types and size of transactions undertaken or policies underwritten by a customer;
        c) The frequency of transactions or duration of the business relationship.

3. The assessment of risks must take into account the prevailing risks identified through the risk assessment at the national level.

4. Licensed entities must examine the factors and variables to determine what the level of overall risk is and take effective actions to mitigate the identified risks. For a higher level of risk, enhanced due diligence measures or risk mitigation measures must be applied, and for a lower level of risk licensed entities may apply simplified customer due diligence, provided there is no suspicion of money laundering or terrorism financing or other specific high risk scenario.

5. Licensed entities must identify and assess the money laundering and terrorism financing risks that may arise from the development of a new product, business practice or delivery mechanism, and

from the use of a new or developing technology for new or pre-existing products. The risk assessment must be carried out prior to the launch of the new product, business practice or prior to the use of the new or developing technology. Licensed entities must take appropriate measures to manage and mitigate the identified risk.

6. Licensed entities may differentiate the extent and depth of application of customer due diligence measures depending on the types and levels of risk for the various risk factors. To this end, licensed entities must assign a risk classification to each customer or group of customers. Licensed entities must be able to demonstrate to the CMA, based on their risk assessment and classification that the customer due diligence measures applied are commensurate to the level of risk identified.

Article 4

Apart from the instances defined in Article 36 (c) and (d), and Article 41 (b) and (d) of the Law, licensed entities must apply enhanced due diligence measures where they otherwise consider, based on a risk assessment or any other information available, that the risk of money laundering or terrorism financing is higher. Possible indicators for situations of higher risk include but are not limited to the following:

1. Customer risk factors:
   a) The business relationship is conducted in unusual circumstances.
   b) Non-resident customers and/or beneficiaries.
   c) The use of front persons or entities (e.g. corporations, trusts);
   d) Legal persons or arrangements that are personal asset management vehicles.
   e) Companies that have nominee shareholders or shares in bearer form.
   f) Businesses or activities that are cash intensive.
   g) The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.
   h) Dealings with financial institutions and intermediaries or customers and/or beneficiaries operating in jurisdictions with ineffective systems for combating money laundering or financing of terrorism, as identified in Clause(2) of this Article.
   i) Politically exposed persons ("PEP"), which includes any natural person, whether as customer or beneficial owner, who is or was entrusted with
      (i) a prominent public function in the Sultanate of Oman or in a foreign country, such as Head of States or of governments,
      (ii) senior politicians,
      (iii) senior government employee,
      (iv) Senior judicial or military officials,
      (v) senior executives of state owned corporations,
      (vi) important political party officials;
      (vii) a prominent function by an international organization, such as directors, deputy directors and members of the board.

The term also includes close associates and family members up to second degree of a politically exposed person and widely and publicly known close business colleagues or personal advisors or any persons who are in position to benefit significantly from close business associations with the politically exposed person.

j) High net worth customers and/or beneficiaries whose source of income is unclear.
k) Customers and/or beneficiaries with criminal, civil or regulatory proceedings against them for crime, corruption, or misuse of public funds, or customers associated with such persons.
l) Customer and/or beneficiary resides in or whose primary source of income originates from a high-risk jurisdiction. Customer's income and/or source of funds/wealth do not match volume or size of premium payments.
m) Customer transfers the contract to another insurer within short period of time.
n) Insurer is made aware of a change in beneficiary only when the claim is made.
o) Customer incurs a high-cost by seeking early termination of the policy.
p) Customer's request to change or increase the sum insured and/or the premium payment are unusual or excessive.

2. Country or geographic risk factors:
   a) Countries classified by credible sources, such as mutual evaluation reports or published follow-up reports, as not having adequate AML/CFT systems.
   b) Countries identified by the Committee as high risk.
   c) Countries subject to sanctions, embargos or similar measures issued by the United Nations.
   d) Countries classified by credible sources as having significant levels of corruption or other criminal activity.
   e) Countries classified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

3. Product, service, transaction or delivery channel risk factors:
   a) Products distributed across via other party distributors or intermediaries in multiple jurisdictions.
   b) Transactions or policies involving accounts in multiple jurisdictions.
   c) Intermediary or distributor is based in, or associated with, jurisdictions with higher money laundering or terrorist financing risk.
   d) Customers or business introduced from one intermediary to another without adequate customer due diligence/know your customer (CDD/KYC) investigations or from high risk jurisdictions.

e) Premiums and/or settlements are paid through accounts held with financial institutions established in jurisdictions associated with higher money laundering or terrorist financing risks.
f) Non-face-to face business relationships initiated without sufficient safeguards, such as certified electronic identification schemes.
g) Anonymous transactions.
h) Insurance Policies, business relationships or transactions conducted with customers that are not physically present for the purpose of identification.
i) Payment received from or channelled to unknown or unassociated other parties.
j) High-value or unlimited value premium payments, overpayments or large volumes of lower value premium payments.
k) Large single premium payments.

Article 5

Enhanced customer due diligence measures may include but are not limited to the following:

1. To obtain additional information on the customer and the beneficial owner(s).
2. To update more regularly the information on the customers and beneficial owners.
3. To obtain information on the reasons for intended or performed transactions or the source of funds or source of wealth of the customer or where necessary the beneficial owner(s).
4. To obtain the approval of senior management to commence or continue the business relationship.
5. To conduct enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
6. To adopt other measures as may be prescribed by the Committee.

Licensed entities must apply enhanced customer due diligence measures to higher risk customers at each stage of the customer due diligence process and on an ongoing basis.

Article 6

Licensed entities may apply simplified customer due diligence measures in situations where a lower risk has been identified in the businesses risk assessment conducted under Article3 of these Instructions or on the national level. The simplified measures taken must be such that they enable the licensed entities business to properly manage and mitigate the prevailing risks. In cases of a money laundering or terrorism

financing suspicion or when specific higher risks scenarios apply, simplified customer due diligence measures must not be permitted. Lower risk situations may include but are not limited to the following:

1. Customer risk factors

   a) Long business relationship with customer with track record of regular premium payments in line with customer profile and source of funds.
   b) Customer was directly identified and on boarded by licensed entity, without involvement of other party intermediaries.
   c) Financial institutions or non-financial businesses and professions that are effectively supervised or monitored to ensure compliance with the requirements of the law.
   d) Companies listed on the stock exchanges of countries with disclosure requirements consistent with international standards, to ensure adequate transparency of beneficial ownership, or majority-owned subsidiaries of such companies.
   e) Public administrations or enterprises.

2. Country or geographical risk factors:

   a) Countries classified by credible sources as having effective systems to combat money laundering and financing of terrorism.
   b) Countries classified by credible sources as having a low level of corruption or other criminal activity.

3. Product, service, transaction or delivery channel risk factors:

   a) Where cash withdrawals are not permitted.
   b) Where redemption or withdrawal of proceeds are not permitted to be paid to other party.
   c) Where it is not possible to change the characteristics of insurance products or policies at a future date to enable payments to be received from, or made to, other parties.
   d) Insurance products that provide benefits similar to retirement to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of members' interests under the scheme.
   e) Insurance benefit only pays out against a pre-defined event or date.
   f) No surrender value.
   g) Low, regular premium payments.
   h) No other party payment facility.
   i) No early surrender option.
   j) Total investment is curtailed at low value.

Article 7

Simplified customer due diligence measures must take into account the nature of the lower risk and be commensurate with the lower risk factors.

Simplified measures may include but are not limited to the following:

1. Obtaining the relevant identification data from a public register, from the customer or from other reliable sources.
2. Verifying identity of customer and beneficial owner(s) after establishment of the business relationship.
3. Postponing the identification of the beneficiary to a later time after their designation.
4. Reducing frequency of customer identification updates .
5. Reducing degree of on-going monitoring and scrutinizing transactions.
6. Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Chapter 3

Due Diligence Measures

Article 8

Licensed entities must refrain from opening or maintaining anonymous accounts or policies, or accounts or policies under fictitious names, numbers or secret codes, or providing any services for such accounts or policies.

Article 9

1. Licensed entities must undertake customer due diligence in the following circumstances:

   a) Before establishing a business relationship;
   b) Whenever there is a suspicion of money laundering or terrorism financing;
   c) Whenever doubts exist about the veracity or adequacy of previously obtained customer identification data or documents.

2. Licensed entities must identify and verify the identity of the customer based on reliable, independent source documents, data or information issued by official authorities.

3. Licensed entities must identify and verify the identity of any person purporting to act on behalf of the customer.

4. Licensed entities must obtain the following unexpired and official documents to satisfy the identification requirements of this Article :

   a) Civil card for Omani nationals or non-Omani residents;
   b) Passport or travel document for persons not residing in the Sultanate of Oman;
   c) Commercial license and registration certificates issued by the Ministry of Commerce, Industry and Investment Promotion for resident companies and establishments or, in the case of non-resident companies and establishments, official documents issued by competent authorities in the country in which they were incorporated or established;
   d) Documents proving that a person has been appointed to represent the customer
   e) For customers not mentioned above, licensed entities must obtain approved official identification documents attested by competent official authorities or bodies that issue the documents.

5. Licensed entities must apply any additional or specific identification and verification requirements prescribed by the CMA, including for state bodies, agencies and public corporations, and for non-profit or non-governmental organizations and other organizations or associations.

6. In all cases, licensed entities shall, as part of the customer due diligence process, take the required measures to understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

Article 10

1. Licensed entities must determine if a customer is acting on behalf of one or more beneficial owners. Such measures must involve obtaining a signed affidavit from the customer at the time of opening the account or establishment of the business relationship or whenever customer due diligence is carried out. The licensed entities must resort to additional reliable sources of information as it deems necessary.

2. If a licensed entity determines that the customer is acting on behalf of one or more beneficial owners, it must identify and take reasonable measures to verify the identity of the beneficial owner(s) using the relevant information or data obtained from a reliable source such that the licensed entity is satisfied that it knows who the beneficial owner(s) is/are. This requirement applies also to accounts opened by lawyers or law firms or other legal professionals on behalf of their clients. Licensed

entities should apply customer due diligence measures on the beneficial owner(s) in this case.

3. If a customer is a company listed on stock exchange of a country with disclosure requirements consistent with international standards, to ensure adequate transparency of beneficial ownership, or a majority-owned subsidiary of such a company, a licensed entity is not required to identify and verify the identity of any shareholder or beneficial owner of the company. In this case, licensed entities shall only obtain customer identification documents on the company itself.

Article 11

1. For customers that are natural persons, licensed entities must obtain the following information as part of the identification and due diligence measures:
   a) Legal name;
   b) Permanent address;
   c) Telephone number, fax number and email address;
   d) Date and place of birth;
   e) Nationality;
   f) Occupation, public position held and/or name of employer;
   g) Civil number as stated in Clause (4) under Article 9 above;
   h) Where the customer is acting on behalf of another person, the name of the beneficiary.
   i) Signature;
   j) Type of account, product or service.
   k) Other relevant information to understand the intended purpose and nature of the business relationship.

2. Licensed entities must verify the information by one or more of the following methods:

   a) Confirming the name and date of birth using an official document as per Article 9 above;
   b) Confirming the permanent address through utility bills, tax assessments, bank statements, or a letter from a public authority;
   c) Contacting the customer by landline telephone, letter or email to confirm the information supplied;
   d) Confirming the validity of the official documents provided under Article 9 through certification by an authorized person.

Article 12

1. For customers that are legal persons, licensed entities must obtain the following information as part of the identification and due diligence measures:

   a) Name, legal form ;
   b) Date and place of incorporation;
   c) Place of management/operations;
   d) The powers to regulate and bind the legal person;
   e) The names of any natural person(s) who directly or indirectly own(s)a controlling ownership interest in the legal person, as well as the names of all persons having senior management positions in the legal person;
   f) The address of the registered office and, if different, a principal place of business;
   g) Official contact information;
   h) Type of account, product or service and
   i) Other relevant information to understand the intended purpose and nature of the business relationship.

2. Licensed entities must verify the information through one or more of the following methods:

   a) Confirm name, legal form and proof of existence of the legal person through reliable documents issued by official authorities;;
   b) a memorandum or articles of association of the legal entity;
   c) For established companies, review a copy of the latest financial reports and accounts;
   d) Conducting an enquiry by a business information service, or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
   e) Conducting enquiring to see that the legal entity has not been, or is not in the process of being dissolved, struck off, wound up or terminated;
   f) Utilizing an independent information verification process, such as by accessing public and private databases;
   g) Obtaining bank references from domestic banks or a bank in a country classified by credible sources as having effective systems to combat money laundering and financing of terrorism;
   h) Contacting the legal persons by landline telephone or email.

Article 13

Licensed entities must understand the nature of the customer's business and its ownership and control structure. Licensed entities must also identify and take reasonable measures to verify the identity of:

1. The natural person or persons who ultimately have a controlling ownership interest in the legal person; or

2. If there is doubt as to whether the person with a controlling ownership interest is indeed the beneficial owner, or where no natural person exerts control through ownership interests, the natural person exercising control of the legal person through other means; or
3. In the absence of any natural persons who have a controlling ownership or otherwise exercise effective control of the legal person, the natural person(s) who hold the position of senior managing official(s).
4. Any natural person, who ultimately has a controlling ownership interest in a legal person of 25% or more, including any natural person that exercises such control or ownership through a chain of ownership, or by means of control other than direct control, is considered to be a "person with a controlling ownership interest".

Article 14

1. When opening an account for or providing services to a trust or other legal arrangement, licensed entities must obtain the following information as part of the identification and due diligence measures:

   a) Name, legal form and proof of existence of the trust or other legal arrangement;
   b) Powers that regulate and bind the trust or other legal arrangement;
   c) Names of all trustees or persons with equivalent positions;
   d) Mailing address;
   e) Contact telephone and fax numbers;
   f) Official identification number, if available (e.g. tax identification number);
   g) Description of the purpose/activities of the trust or other legal arrangement; and
   h) Other relevant information to understand the intended purpose and nature of the business relationship.

2. Licensed entities must take reasonable measures to verify the information through one or more of the following methods:

   a) Obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
   b) Obtaining bank references from a domestic bank or a bank in a country classified by credible sources as having effective systems to combat money laundering and financing of terrorism;
   c) Accessing public and private databases or official sources.

Article 15

Licensed entities must identify and take reasonable measures to verify the identity of:

1. Trustees, managers, board of directors or persons in equivalent positions;
2. Settlors, founders or persons in equivalent positions;
3. The trust or other legal arrangement, including any persons settling assets into the trust or other legal arrangement, including through a chain of control or ownership;
4. The officer exercising ultimate effective control over the trust or other legal arrangement;
5. Beneficiaries or other legal arrangement, the licensed entities must obtain sufficient information concerning the beneficiaries to satisfy the entity that it will be able to establish the identity of the beneficiaries at the time of the payout or when the beneficiary intends to exercise vested rights; and
6. Signatories.

Article 16

1. In addition to carrying out customer due diligence on the customers and beneficial owners, licensed entities must conduct the following measures as on the beneficiary or beneficiaries of the policy as soon as the beneficiary or beneficiaries have been identified or designated:

a) For a beneficiary that is identified by name, take the name of that person;
b) For a beneficiary that is designated by characteristics, class or by other means, obtain sufficient information on the beneficiary so that licensed entity is satisfied that it is able to establish the identity of the beneficiary at the time of payout; and
c) Verify the identity of the beneficiary prior to the payout of the policy.

2. Licensed entities must include the beneficiary of a life insurance policy as a relevant risk factor in determining whether enhanced CDD measures are applicable.

3. If a licensed entity determines that, a beneficiary of a policy is a legal person or legal arrangement that presents a higher risk, the licensed entity must take enhanced due diligence measures and take reasonable measures to identify and verify the identity of the beneficial owner(s) of the beneficiary prior to the time of payout.

Article 17

Licensed entities must take reasonable measures to determine prior to the time of payout whether the beneficiary or beneficiaries or the beneficial owner(s) of a beneficiary is a politically exposed person and if so, the licensed entity must:

a) Inform senior management before the payout of the policy proceeds;

b) Conduct enhanced due diligence and scrutiny on the whole business relationship with the policy holder; and
c) Consider making a report to the Centre.

Article 18

Licensed entities must ensure that documents, data or information collected in accordance with this Chapter are kept up-to-date and relevant by undertaking reviews of existing records, particularly of higher risk categories of customers, products or transactions. The frequency and scope of the reviews should be determined on the basis of the risks posed.

Chapter 4

Ongoing Preventive Measures

Article 19

Licensed entities must conduct due diligence on business relationships and review existing records on an ongoing basis to ensure that documents, data or information collected under the due diligence process are kept both up-to-date and relevant, particularly for higher risk customers. Financial Institutions shall furthermore adopt automated systems to monitor and scrutinize customer transactions throughout the course of the business relationship to ensure that they are consistent with the licensed entity's knowledge of the customer and the customer risk profile and, where necessary, the source of funds and wealth.

Article 20

Licensed entities must apply customer due diligence measures to customers, beneficial owners and beneficiaries with which they had a business relationship at the time of the coming into force of these Instructions. The measures must be applied at appropriate times and based on materiality and risk, and taking into account whether and when customer due diligence measures have previously been undertaken and the adequacy of the data obtained.

Article 21

Licensed entities must apply enhanced customer due diligence measures for business relationships or transactions with a person who is not physically present for the purpose of identification. Such measures may include applying additional verification measures and where appropriate, requesting additional or certified documents or applying other safeguards, such as certified remote electronic identification schemes.

Article 22

Where a licensed entity is unable to comply with the required customer due diligence measures, it must refrain from opening the account, issuing a policy, commencing the business relationship or carrying out the transaction or it must terminate the business relationship. In such cases, the licensed entity must consider filing a report with the Centre.

Licensed entities may delay the verification of the customer or beneficial owner(s) identity until after the establishment of the business relationship or carrying out of the transaction, provided all conditions set out in Article 37 of the Law are met. For such situations, licensed entities must include in their risk management procedures to mitigate the risks, for example by limiting the number, types and/or amount of transactions that can be performed, and through close monitoring of large or complex transactions that are being carried out outside the expected norms of that relationship. Verification must be carried out as soon as possible after the establishment of the business relationship.

Article 23

The measures and procedures applied to licensed entities that seek to establish a correspondent relationships pursuant to Article 38 of the Law must be documented in writing and licensed entities must ensure that they clearly understand the respective AML/CFT responsibilities of each institution. The requirements set out in Article 38 of the Law shall apply also to cross border correspondent relationships established prior to the enactment of the Law and issuance of these Instructions. Licensed entities shall not enter into or continue correspondent relationships with shell banks; and shall satisfy themselves that respondent institutions do not permit their accounts to be used by shell banks.

Confidentiality requirements shall not preclude the licensed entity from providing the information or documents required by the financial institution when establishing correspondent relationship to ensure they satisfy term and conditions equal to those provided for in Article (38) of the Law.

Article 24

Licensed entities must examine, as far as reasonably possible, the background and purpose of all large, complicated and unusual large transactions, and all unusual patterns of transactions that do not have an apparent economic or lawful purpose. Where the risk of money laundering or terrorism financing is higher, licensed entities must apply enhanced customer due diligence measures consistent with the risks identified. Such measures must include increasing the degree and nature of monitoring of the business relationship and related transactions.

Article 25

In complying with the obligation in Article 36(d) of the Law, licensed entities shall apply the following, additional measures:

(1) Put in place risk management systems to determine whether a customer or beneficial owner is a PEP or a family member or close associate of a PEP;

(2) obtain senior management approval before establishing or continuing an existing business relationship involving a customer or beneficial owner that is a PEP, or a family member or close associated of a PEP;

(3) take reasonable measures to determine the source of funds and wealth of the customer or beneficial owner identified as PEPs, or as a family member of close associate of a PEP; and

(4) conduct enhanced ongoing monitoring on the business relationship.

Article 26

1. Licensed entities must examine all transactions and business relations with natural and legal persons or financial institutions from countries which have been identified by the Committee pursuant to Article 13 (k) of the Law, and must apply risk based or enhanced measures that are effective and proportionate to the risks involved. Licensed entities must also apply the counter-measures prescribed by the Committee in relation to higher risk countries.

2. Licensed entities shall regularly check the Committee's updates to the lists of high risk countries and the required measures to be taken in relation to each country.

3. Licensed entities are prohibited from accepting cash transactions or carrying out cash transactions for their customers for life insurance policies except through the banking system or electronic payment means.

Article 27

Licensed entities must maintain records of the following information:

1. Copies of all records, documents, information, and data obtained through the customer due diligence process including documents evidencing the identities of customers and beneficial owners as well as beneficiaries, account and policy files and business correspondence, for at least ten (10) years after the business relationship has ended or a transaction with a customer who does not have an established business relationship with the licensed entities business has been carried out.
2. All records of transactions, both domestic and international, attempted or executed for at least ten (10)years following the attempt or execution of the transaction. Such records must be

sufficiently detailed to permit the reconstruction of each individual transaction so as to provide, if necessary, evidence for prosecution of criminal activity; and be kept in official records following a regular accounting system.

3. Copies of suspicioustransaction reports sent to the Centre and related documents for at least ten (10) years after the date the report was made to the Centre.
4. The risk assessment reports and any underlying information for a period of five (5)years from the date the assessment was carried out or updated.

Licensed entities must keep the records, documents, information, and data in a way that they can immediately be made available to the competent authority or the CMA.

Chapter 5

Internal Policies, Controls and Procedures

Article 28

Licensed entities must develop and implement policies, controls and procedures that ensure that they are complying with the provisions of the Law, these instructions and any other instructions issued by the CMA. Such policies, controls and procedures must be approved by the board of directors of the licensed entity and must be adequate to enable the licensed entity to manage and mitigate the risks that have been identified either on the national level or by the licensed entity. Licensed entities must monitor the implementations of those policies, controls and procedures and enhance them, if and as necessary. Such policies, controls and procedures must address, at a minimum, the following:

1. Risk assessment procedures in line with Article 34 of the Law and Chapter 2 above, including for new and existing customers, beneficial owners as well as of transactions and the business as such.
2. Procedures to identify and verify the identity of and apply full customer due diligence to customers, beneficial owners in line with Chapter 3 above.
3. Procedures to maintain records and information of customers, beneficial owners, , business relationships and transactions in line with Article 27 above.
4. Procedures for identifying suspicious transactions/activities and for reporting such transactions/activities to the Centre pursuant to Article 47 of the Law.
5. External audit function to ensure that internal policies, procedures, systems and controls are subject to independent testing and review.
6. Procedures for appointing a compliance officer at senior management level to ensure compliance by the licensed entity with the provisions of the Law and this Instructions.
7. Screening procedures to maintain high standards when recruiting employees.

8. On-going training programs for all new and existing employees, directors, board members, and executive or supervisory management to keep them informed of all aspects of legal requirements, new developments and money laundering and terrorism financing techniques, and to help them detect transactions and activities that may be connected to money laundering, predicate offences or terrorism financing, and familiarize them with the procedures to be followed in such cases.
9. Other arrangements as prescribed by the CMA.

Article 29

1. AML/CFT policies, controls and procedures should be applicable and appropriate to all branches and majority owned subsidiaries of the financial group. In addition to elements mentioned in Article 28 of these Instructions, the AML/CFT policies, controls and procedures should contain:

(a) Policies and procedures for sharing information for the purposes of CDD and ML/TF risk management;
(b) The provision, at group level compliance, audit and AML/CFT functions, of customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions and activities which appear unusual, including suspicious activity and transaction reports and underlying information;
(c) Adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off.
2. In the case of their foreign operations, where the minimum requirements of the host country on anti-money laundering and combating the financing of terrorism are less strict, licensed entities must ensure that their branches and majority-owned subsidiaries in host countries implement the requirements stipulated by the Law and Regulations to the extent that host country laws permit. If the host country does not permit the proper implementation of the measures above, the licensed entity should apply appropriate additional measures and inform the CMA.

Article 30

1. As part of their internal controls and procedures under Article 42 of the Law and Article 28 above, licensed entities must appoint a compliance officer at the senior management level who is responsible for the licensed entities' compliance with and implementation of its obligations. The compliance officer and any other compliance staff must have timely access to customer identification data and other customer due diligence information, transaction records, and other relevant information. The compliance officer must have appropriate experience and qualifications in the field of anti-money laundering and combating the financing of terrorism and have the authority to act independently and to report to senior management.

2. The licensed entities must supply the CMA and the Centre with details of the compliance officer, including name, qualifications, contact number and email address and must promptly inform the

CMA and the Centre of any change of compliance officer. This includes providing the CMA and the Centre with details of the deputy compliance officer in cases where the compliance officer is suspended for specific period of time.

Article 31

The compliance officer must periodically report to the board of directors or partners meeting. The latter must review the licensed entity's compliance with the requirements of the Law and these instructions. Written reports to the board of directors or partners meeting shall be submitted at least quarterly and must include a statement on all suspicious transactions detected and how it has been handled, implications and measures taken by compliance staff to strengthen the businesses' anti-money laundering and combating the financing of terrorism policies, procedures, systems and controls. The particulars of the suspected person or any indication thereto shall not be mentioned in the reports.

Article 32

Licensed entities must maintain an adequately resourced and independent audit function to ensure that the compliance officer and all staff are performing their duties in accordance with their internal policies, procedures, systems and controls and in compliance with the requirements of the Law and these Instructions.

Article 33

Licensed entities must define fit and proper requirements and a code of conduct for all of its employees, directors, board members and executive or supervisory management. In addition, licensed entities must establish screening procedures to ensure appropriate standards when hiring employees, directors, board members and executive or supervisory management. Such screening procedures must ensure that:

1. Employees, directors, board members and executive or supervisory management have the high level of competence necessary for performing their duties; and
   have appropriate ability and integrity to conduct the business activities of the licensed entity;
2. Potential conflicts of interests are taken into account, including the financial background of the employees, directors, board members and executive management; and
3. Persons charged or convicted of offences involving fraud, dishonesty or other similar offences are not employed or discharged of their duties.

Chapter 6

Article 34

1. Licensed entities' managers, members of the board of directors, owners, authorized representatives, employees, agents, and partners and must promptly notify the compliance officer of any unusual or suspicious transaction. The compliance officer or any other person so authorized must promptly file a suspicious transaction report (STR) with the Centre if there is a suspicion, or there are reasonable grounds to suspect, that funds are the proceeds of crime, or are related to terrorism financing. The reporting shall occur as soon as possible but no later than 24 hours after forming a suspicion or having reasonable grounds to suspect that any transaction or attempted transaction, regardless of its value, involves proceeds of crime or funds related to terrorism financing. STRs must include all relevant information, documents and records relating to the transaction, customer or account involved, and comply with the procedures and requirements set out by the Centre.

2. The compliance officer shall, without delay, consider whether a suspicion or reasonable grounds to suspect, referred to in Article 34(1) of these Instructions, arise, following the receipt of information or notification from managers, members of the board of directors, owners, authorized representatives, employees, agents, partners, and professionals appointed to perform any tasks on their behalf, of the licensed entity.

The requirement under this provision is subject to the non-disclosure requirement under article 49 of the Law, according to which the reporting person shall not reveal to the customer, beneficial owner or any other party that they have issued or are about to issue a report to the Center, or give any information or data in relation to such reports or alert them to any investigation in that regard.

Article 35

Licensed entities must provide any relevant information or documents or files, however stored, regarding any requests received from the competent entity, including requests unrelated to a previously filed suspicious transaction report, provided that it relates to a suspicion of money laundering or terrorism financing, and within the time frame prescribed by the Centre or the competent entity, as the case may be.

Article 36

In cases where licensed entities form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, they should not pursue the CDD process, and instead should file a report to the Center. The protection prescribed under Article (47) of the Law shall apply also in cases where the licensed entity does not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

Chapter 7

Reliance on Third Parties for Client Due Diligence Purposes

Article 37

1. Licensed entities may rely on a third party to perform identification and verification of the customer; or the beneficial owner; or to take the required measures to understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

2. If licensed entities place reliance on a third party, they shall:

   a. Immediately obtain all necessary information on the identity of the customer and/or beneficial owner and/or the purpose and intended nature of the business relationship as required under the Law and this Instruction;
   b. Take steps to satisfy themselves that copies of the identification data and other relevant documentation relating to customer due diligence requirements will be made available from the third party upon request and without delay; and
   c. Satisfy themselves that the third party is regulated and supervised for and has measures in place for compliance with customer due diligence and record keeping requirements in line with the obligations stipulated in the Law and these Instruction.
   d. The ultimate responsibility for all requirements stipulated herein remain with the licensed entity relying on the third party.

3. When determining in which countries the relied upon third party may be based, licensed entities shall have regard to information available on the level of country risk and to the instructions issued by the Committee pursuant to Article 13 (k) of the Law.
4. Licensed entities that rely on third parties that are part of the same financial group may consider that the third party relied upon meets the requirements under this Article, provided the group applies due diligence and record keeping requirements in line with the Law and this Instruction, the implementation of such requirements is supervised at the group level by a competent authority, and any higher country risk is adequately mitigated by the group's policies and controls.

5. Where a correspondence relationship is established between the licensed entity and a foreign financial institution and the foreign financial institution relies on an Omani third party to carry out CDD measures, the confidentiality requirements shall not preclude the licensed entity from providing to the foreign financial institution the information and documents required to meet its legal obligations in its home country regarding relying on a third party.

6. This Article shall not apply to outsourcing services and agency relationships where, on the basis of a contract, the outsourcing service provider, intermediary or agent applies CDD measures on behalf of the financial institution, in accordance with its procedures, and is subject to the delegating financial institution's control in relation to the effective implementation of the CDD requirements

Chapter 8

Final Provisions

Article 38

The Licensed entity shall comply with the decisions of the National Committee for Combating Terrorism and the United Nations Security Council's Resolutions Issued under Chapter VII of the United Nations Charter on the Prevention and Suppression of Terrorism and the Financing of Terrorism and prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing.

Article 39

Notwithstanding any punishments in the law, any person breaching these instructions shall be punished by one or more of the measures and penalties stipulated in Article (52) of the Law.