Instructions for all Licensed Financial Institutions under the Supervision of Central Bank Of Oman on implementing Combating Money Laundering and Terrorism Financing Law (30/2016)

These Instructions are issued by the Central Bank of Oman pursuant to its powers under the Banking Law no. 114/2000, and in its capacity as a Supervisory Authority pursuant to Article 51(c) of the Law on Combating Money Laundering and Terrorism Financing no. 30/2016. Financial institutions are required to comply with all applicable provisions of these Instructions. All other relevant instructions previously issued by the Central Bank of Oman, shall still be in force unless inconsistent with these instructions.

Article 1

The definitions set out in Article 1 of Law No. 30/2016 on Combating Money Laundering and Terrorism Financing Law shall apply to these instructions. In implementation of the provisions of these Instructions, the following terms and expressions shall have the meanings indicated below, unless the context requires otherwise:

AML: Anti-Money Laundering

CFT: Combating the Financing of Terrorism

FATF: Financial Action Task Force

Committee: The National Committee for Combating Money Laundering and Terrorism Financing.

Center: The National Center for Financial Information

Law: Combating Money Laundering and Terrorism Financing Law (30/2016)

The terms 'prominent position', 'members of their family' and 'close associates' in Article 36 of the Law should be interpreted to include any natural person, whether as customer or beneficial owner, who is or was entrusted with a prominent public function in the Sultanate of Oman or in a foreign country, such as Head of States or of governments, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials; or entrusted with a prominent function by an international organization, such as directors, deputy directors and members of the board. The terms also include immediate family members and close associates. Close associates includes 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. Family members include the parents, siblings, children, spouse and in-laws of a politically exposed person.

Chapter 1 – Risk Assessment

Article 2

(1) Pursuant to Article 34 of the Law, financial institutions should assess the money laundering and terrorism financing risks inherent to their business. The risk assessment and any underlying information shall be documented in writing, be kept up-to-date and readily available for the Central Bank of Oman to review upon request. In assessing money laundering and terrorism financing risks, financial institutions should give consideration to all relevant risk factors, which may include but are not limited to:

- Customer risk;
- Countries or geographic area in which customer operates or the place of origination or destination of a transaction;
- The nature of products, services and transactions offered and the delivery channels for products and services.

For all categories, financial institutions should 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:

i. The purpose of an account or relationship;
ii. The size of deposits or transactions undertaken by a customer;
iii. The frequency of transactions or duration of the relationship.

The assessment of risks should also take into account the prevailing risks identified through the risk assessment prepared on the national level. Financial institutions should examine the factors and variables to determine what is the level of overall risk and the appropriate level of mitigation to be applied. For higher level of risks enhanced due diligence measures should be applied, and for a lower level of risks financial institutions may, subject to any conditions specified under Article 40 of the Law, apply simplified customer due diligence, provided there is no suspicion of money laundering or terrorism financing in which case simplified customer due diligence should not be permitted. Financial institutions 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 but, at a minimum, must comply with the provisions of Articles 33, 35, 36, 38, 39, 41 and 44 of the Law

(2) In developing and implementing the risk-based approach pursuant to Article 34 of the Law, financial institutions should establish and maintain a risk profile on customers, based upon sufficient knowledge of the customer and beneficial owner(s), the intended nature of the business relationship with the financial institutions, and on the source of funds. Financial institutions should classify their customers into risk categories, to which differentiated levels of customer due diligence shall be applied by the financial institutions in accordance with the financial institution's assessment of the risk. Financial institutions may develop a system of risk classification or may adopt the following as a minimum set of classifications:

- Low risk, pursuant to Article 3 herein and any conditions set under Article 40 of the Law;
- Normal risk, for customers that do not exhibit the characteristics of either low-risk or high-risk customers;
- High risk (referred to in Annex 1), for which enhanced due diligence measures shall apply pursuant to Annex 2. Financial institutions may provide for additional subcategories of higher risk customers, to which differentiated levels of enhanced due diligence would be applied, consistent with the financial institution's assessment of the risk.

(3) Pursuant to Articles 34(a) and 41(c) of the Law, financial institutions should identify and assess the money laundering and

terrorism financing risks that may arise from the development of a new product, service, business practice or delivery mechanism, and from the use of a new or developing technology for new or pre-existing products or services. The risk assessment shall be carried out prior to the launch of the new product, service, business practice or prior to the use of the new or developing technology. Financial institutions shall take appropriate measures to manage and mitigate the identified risk.

Article 3

Financial institutions should apply simplified customer due diligence measures in situations where a lower risk has been identified under Article 2. The simplified measures taken shall be such that they enable the financial institutions to properly manage and mitigate the prevailing risks. Pursuant to Article 40 of the Law, the Central Bank of Oman, in coordination with the Center, specifies the following conditions for the application of simplified due diligence measures:

(1) In cases of a money laundering or terrorism suspicion, simplified customer due diligence measures shall not be permitted.

(2) Lower risk situations may include the following:

a) Customers:

- Financial institutions or non-financial businesses and professions that are subject to requirements to combat money laundering and terrorism financing consistent with the FATF Recommendations, have effectively implemented those requirements, and are effectively supervised or monitored to ensure compliance with those requirements.
- Public companies listed on a stock exchange and subject to disclosure requirements (either by law, or stock exchange rules or other binding instructions), which impose requirements to ensure adequate disclosure of beneficial ownership.
- Public administrations or enterprises.

b) Products, services, transactions or delivery channels:

- A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of member's interest under the scheme.

- Financial products or services that are of a limited nature that are provided to a certain category of customer for financial inclusion purposes, with the prior approval of the Central Bank of Oman.

Article 4

Simplified customer due diligence measures shall 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:

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship.
- Reducing the frequency of customer identification updates.
- Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.
- 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.

Financial institutions should not apply simplified customer due diligence measures whenever there is a suspicion of money laundering or terrorism financing.

Chapter 2 – Due Diligence Measures

Article 5

Pursuant to Article 35 of the Law, opening or maintaining anonymous accounts or accounts under fictitious names, numbers or secret codes, or providing any services for such accounts remain prohibited.

Article 6

1. Pursuant to Article 33(a) of the Law, financial institutions should undertake customer due diligence in the following circumstances:

a) before establishing a business relationship;
b) before carrying out a transaction for a customer with whom it does not have an established business relationship which value is equal to or greater than **OMR 6000** for transactions carried out in a single stage or multiple stages;
c) before carrying out a wire transfer for a customer with whom it does not have an established business relationship which

value is equal to or greater than **OMR 400** or its equivalent in foreign currency;

d) when there is a suspicion of money laundering or terrorism financing;

e) when there are doubts concerning the veracity or adequacy of previously obtained identification documents and information.

2. Financial institutions should identify and verify the customer based on reliable, independent source documents, data and information issued by public authorities.

3. Financial institutions should identify and verify the identity of any person operating on behalf of the customer and seek proof of the authenticity of their agency according to applicable regulations.

4. For purposes of fulfilling their obligations under subsections (2) and (3), financial institutions should obtain the following unexpired and official documents, according to each specified case, to satisfy the identification requirements as per this Article:

a) Civil card for Omani nationals and non-Omani residents;

b) Passport or travel document for persons not residing in the Sultanate of Oman;

c) Commercial license issued by the Ministry of Commerce and Industry for resident companies and establishments and, in the case of non-resident companies and establishments, documents issued by competent authorities in the state in which they were incorporated or established;
d) Documents, papers, instruments, and court orders proving that a person has been appointed to represent the customer.
e) For customers not mentioned above, financial institutions should have to obtain approved official identification documents attested by competent public authorities or bodies that issue these documents.

Article 7

Financial institutions should identify any person acting on behalf of a customer, verify this person's identity, and whether there the latter is duly authorized to represent the customer. Financial institutions should also identify beneficial owners of business relationships and transactions, and take reasonable measures to verify their identity until financial institutions are satisfied that they know who the beneficial owners are. Such measures should involve, at a minimum, obtaining a signed undertaking from the customer at the time of opening the account or whenever customer due diligence is carried out, stating that the customer is the beneficial owner. The financial institutions shall resort to

additional sources of information, if and as deemed necessary by the financial institutions to be satisfied whether or not the customer is acting on behalf of another or others.

This requirement applies also to accounts opened by lawyers or law offices on behalf of their clients. Financial institutions should apply customer due diligence measures on the beneficial owner(s) in each case.

If a customer is a company listed on a stock exchange, a financial institutions is not required to identify and verify the identity of any shareholder or beneficial owner of the company provided that the company is subject to adequate disclosure requirements to ensure transparency of beneficial ownership. In this case, financial institutions should only obtain customer identification documents on the company itself, subject to the provisions of Article 11 herein.

Article 8

For customers that are natural persons and for beneficial owners, financial institutions should obtain the following information as part of the identification measures:

- Legal name and any other names used;

- Correct permanent address;
- Contact telephone number, fax number and email address, as applicable;
- Date and place of birth;
- Nationality;
- Occupation, public position held and/or name of employer;
- Official personal identification number or other unique identifier contained in a document that bears a photograph of the customer;
- Type of account and nature of the banking relationship;
- Intended purpose and nature of the business relationship; and
- Signature.

Financial institutions should verify the above information by the following methods in order to satisfy the financial institutions of the existence and identity of the natural person or beneficial owner:

- Using an official document;
- In case the indicated permanent address cannot be verified by an official document, it can be confirmed through utility bills, tax assessments, bank statements, or a letter from a public authority;
- In the event the occupation indicated cannot be verified by an official document, it can be confirmed through an official

human resources letter issued by the employer, tax assessments, or any other reliable independent document.

- In case the financial institutions has doubts on the validity of the official document provided, it can confirm the document through certification by an authorized person.

Article 9

For customers that are legal persons, financial institutions should obtain the following information as part of the identification measures:

- Name, legal form and proof of existence;
- The powers to regulate and bind the legal person, as well as the names of all persons having a senior management position in the legal person;
- The address of the registered office and, if different, a principal place of business;
- Contact telephone number, fax number and email address, as applicable;
- Intended purpose and nature of the business relationship;
- Intended purpose and nature of the business relationship; and
- Signatures of all officers of the legal person with signing authority on the account(s).

The financial institutions should verify the above information through the following methods in order to satisfy the financial institutions about the existence and identity of the legal person has been established:

- Confirming name, legal form and proof of existence through a certificate of good standing, a partnership agreement or other documentation from a reliable independent source proving the name, form and current existence of the customer;
- Confirming the powers to regulate and bind the legal person through a memorandum or articles of association, , or equivalent instrument;
- For established companies or other legal persons, reviewing a copy of the latest annual report and accounts;
- Conducting an enquiry by a business information service, or obtaining an undertaking from a reputable and known firm of lawyers and accountants confirming the documents submitted;
- Utilizing an independent information verification process, such as by accessing public and private databases;
- Verifying tax payer card;
- Obtaining prior bank references;

Article 10

In addition to carrying out customer due diligence on the legal person, financial institutions should understand the nature of the customer's business and its ownership and control structure. Pursuant to Article 33(c) of the Law, financial institutions shall identify and take reasonable measures to verify the identity of:

- the natural persons who ultimately have a controlling ownership interest in a legal person; or
- if there is doubt as to whether the persons with controlling ownership interest are indeed the beneficial owners, or where no natural person exerts control through ownership interests, the natural persons exercising control of the legal person through other means; or
- In the exceptional circumstances of an absence of any natural persons who have a controlling ownership or otherwise exercise effective control of the legal person, the natural person who holds the position of senior managing official.

Article 11

When opening an account for a trust or legal arrangement, financial institutions should obtain the following information as part of the identification measures:

- Name, legal form and proof of existence of the trust or legal arrangement;
- The trust deed or other document containing the powers that regulate and bind the trust or legal arrangement;
- Names of all trustees;
- Mailing address of the trustee(s);
- Contact telephone number, fax number and email address of the trustee(s), as applicable;
- Some form of official identification number, if available, for the trust and the trustee(s) (e.g. tax identification number); and
- Description of the purpose/activities of the trust or legal arrangement;
- Intended purpose and nature of the business relationship; and
- Signature of the trustee(s).

Financial institutions should verify the above information, at minimum, through an authenticated copy of the trust or legal arrangement agreement. Additionally, one or more of the following methods can be applied in order to satisfy the financial institutions about the existence and identity of the trust or legal arrangement has been established:

- Obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- Obtaining prior bank references;
- Accessing public and private databases or official sources.

Article 12

When opening an account for a trust or legal arrangement, in addition to carrying out customer due diligence on the trust or legal arrangement, financial institutions should identify and take reasonable measures to verify the identity of:

- Trustees, managers, directors or persons in equivalent positions;
- Settlors, founders or persons in equivalent positions;
- The trust or legal arrangement, including any persons settling assets into the trust or legal arrangement;
- Protectors or persons in equivalent positions and exercising ultimate effective control over the trust;
- Beneficiaries or persons in equivalent positions; and
- Signatories.

Beneficiaries who have not been defined at the time of the establishment of the business relationship with the financial institutions should be identified when they can be so defined and no disbursement should be made by the financial institutions to such beneficiary until they have been identified in accordance with the Law.

Article 13

Pursuant to Article 36(b) of the Law, financial institutions should ensure that documents, data or information collected in accordance with the Law shall be kept up-to-date and relevant by undertaking reviews of existing records, particularly of higher risk categories of customers and transactions.

Article 14

In complying with the obligation in Article 36(a) of the Law, financial institutions should adopt automated systems to monitor on an ongoing basis customer transactions and customer relationships. Monitoring shall include the scrutiny of customer transactions to ensure that they are being conducted according to the financial institution's knowledge of the customer, the customer risk profile, the source of funds and, in higher-risk cases, the source of the customer's wealth.

Chapter 3 – Ongoing Preventive Measures

Article 15

Pursuant to Article 33 of the Law, banks should apply CDD measure to customers and beneficial owners with which it had a business relationship at the time of the coming into force of the Law. The measures shall be applied at appropriate times considering the materiality and risk represented by these relationships.

Article 16

Pursuant to Article 36(c) of the Law, financial institutions should apply enhanced customer due diligence measures for non-face-to-face business relationships or transactions. Such measures may include requesting certification of documents or requesting additional documents; and applying additional verification measures.

Article 17

Pursuant to Article 39 of the Law, where a financial institution is unable to comply with the required identification and verification measures, it should refrain from opening the account or

commencing the business relationship or carrying out the transaction, or it should terminate the business relationship. In such cases, the financial institutions should file a report with the Center.

Financial institutions may delay the verification of the customer or beneficial owner 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. Financial institutions shall include in their risk management procedures to mitigate the higher risk in such situations, for example a limitation of the number, types and/or amount of transactions that can be performed, and close monitoring of large or complex transactions being carried out outside the expected norms of that type of relationship. Verification shall be carried out as soon as possible after the establishment of the business relationship.

Article 18

The requirements for financial institutions relating to correspondent banking relationships set out in Article 38 of the Law shall be documented in writing and be applied to cross border correspondent banking relationships established prior to the enactment of the Law and issuance of these Instructions.

Article 19

Financial institutions should examine, as far as reasonably possible, the background and purpose of all 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, financial institutions should apply enhanced customer due diligence measures consistent with the risks identified. Such measures should include increasing the degree and nature of monitoring of the business relationship and related transactions to determine whether those transactions or activities appear unusual or suspicious.

Article 20

Pursuant to Article 41(d) of the Law, financial institutions should examine all transactions and business relations with persons and financial institutions from countries which have been identified by the Committee pursuant to Article 13 (K) of the Law, and should apply enhanced due diligence measures that are effective and proportionate to the risks involved. Financial institutions should also apply the measures prescribed by the Committee in relation to such higher risk countries.

Article 21

Pursuant to Article 44 of the Law, financial institutions should maintain records of the following information:

a) 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, account files and business correspondence, for at least ten years after the business relationship has ended or a transaction with a customer who does not have an established business relationship with the financial institutions has been carried out.
b) All records of transactions, both domestic and international, executed for at least ten years following the execution of the transaction. Such records must be sufficiently detailed to permit the reconstruction of each individual transaction and be kept in official records following a regular accounting system.
c) Copies of transaction reports sent and related documents for at least ten years after the date the report was made to the Centre.
d) The risk assessment and any underlying information for a period of ten years from the date the assessment was carried out or updated.

Financial institutions should keep the records, documents, information, data, or certified copies of those thereof, in a way that they can immediately be made available to judicial authorities, the Center, and supervisory authorities, upon demand.

Chapter 4 – Internal Policies, Controls and Procedures

Article 22

Pursuant to Article 42 of the Law, financial institutions should develop and implement AML/CFT policies, controls and procedures that ensure that they are complying with the provisions of the Law, this and any other Instructions issued on the basis of the law, and any relevant decisions and instructions issued by the Central Bank of Oman and the Center. Such policies, controls and procedures shall be approved by the financial institution's board of directors or senior management and allow for any identified risks to be managed and mitigated effectively. Financial institutions shall monitor the implementations of those policies, controls and procedures and enhance them, if and as necessary. Such policies, controls and procedures shall address, at a minimum, the following:

a) Risk evaluation procedures of new and existing customers and beneficial owners, as well as of transactions.

b) Procedures to identify and verify the identity of and apply full customer due diligence to customers and beneficial owners.
c) Procedures to maintain records and information of customers, beneficial owners, business relationships and transactions.
d) Procedures for reporting to the Centre suspicious transactions pursuant to Article 47 of the Law.
e) Independent audit function to ensure that internal policies, procedures, systems and controls are subject to independent testing and review.
f) Procedures for appointing a compliance officer at senior management level to ensure compliance by the financial institutions with the provisions of the Law and these Instructions.
g) Screening procedures to maintain high standards while recruiting employees.
h) 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 AML and CFT 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.

i) Mechanisms to share information with other members of the banking group and to protect its confidentiality and to grant group-level compliance, audit and other AML/CFT functions with full access to customer, account, and transaction information from branches and subsidiaries for AML/CFT purposes and mechanisms to adequately safeguard the confidentiality and use of information exchanged.
j) Other arrangements as prescribed by the Central Bank of Oman.

Article 23

AML/CFT policies, controls and procedures should be applied to all domestic and foreign branches and majority-owned subsidiaries of the banking group.

In the case of their foreign operations, where the minimum AML/CFT requirements of the host country are less strict than those stipulated by the Law and subsequent instructions, financial institutions should ensure that their branches and majority-owned subsidiaries in host countries implement the requirements stipulated by the Law and subsequent instructions, to the extent

that host country laws and regulations permit. If the host country does not permit the proper implementation of the measures above, financial groups should apply appropriate additional measures to manage the money laundering and terrorist financing risks, and inform the Central Bank of Oman.

Article 24

As part of their internal AML/CFT controls and procedures, financial institutions should appoint a compliance officer at the senior management level who is responsible for the financial institution's compliance with and implementation of its AML/CFT obligations. The compliance officer and any other compliance staff shall have timely access to customer identification data and other customer due diligence information, transaction records, and other relevant information. The compliance officer should have appropriate experience and qualifications in the field of AML/CFT and have the authority to act independently and to report to senior management.

The financial institutions should supply the Central Bank of Oman and the Center with details of the compliance officer, including name, qualifications, contact number and email address. The financial institutions shall promptly inform the

Central Bank of Oman and the Center of any change of compliance officer.

Article 25

The compliance officer should periodically report to the Board of Directors and the Board of Directors shall review the financial institution's compliance with the requirements of the Law and these Instructions. Such regular reports to the Board of Directors shall include summaries and statistics on compliance officer's activities regarding reporting suspicious transactions detected and how they have been handled, measures taken by compliance staff and any additional steps needed to strengthen the financial institution's AML/CFT policies, procedures, systems and controls. The periodic compliance reports should include an assessment of the adequacy of the financial institution's human resources and automated information systems available for AML/CFT compliance and provide an overall assessment of the effectiveness of the AML/CFT program implemented in the financial institution. The periodic compliance reports should be made available to the Central Bank of Oman, upon request.

Article 26

Financial institutions should maintain an adequately resourced and independent audit function which shall conduct testing to

assess whether the compliance officer and financial institution's staff are performing their duties in accordance with the financial institution's AML/CFT internal policies, procedures, systems and controls and in compliance with the Law and these Instructions.

Article 27

Pursuant to Article 42(b) of the Law, financial institutions should establish ongoing employee training to ensure that new and existing employees, including directors, board members, executive or supervisory management, compliance officer(s) and internal auditor(s) are kept informed of new developments, including typologies on current money laundering and terrorism financing and their obligations under the Law, these Instructions and any other laws and instructions relevant to AML/CFT.

Article 28

Financial institutions should develop and apply policies and procedures to implement fit and proper requirements and a code of conduct for all of its employees, directors, board members, executive or supervisory management, compliance officer(s) and internal auditor(s). In addition, financial institutions should establish screening procedures to ensure appropriate standards when hiring employees, directors, board members and executive

or supervisory management. Such screening procedures shall ensure that:

- Employees, directors, board members and executive or supervisory management, compliance officer(s) and internal auditor(s) have the high level of competence necessary for performing their duties;
- Employees, directors, board members and executive or supervisory management, compliance officer(s) and internal auditor(s) have appropriate ability and integrity to conduct the business activities of the financial institutions;
- Potential conflicts of interests are taken into account, including the financial background of the employees, directors, board members , executive or supervisory management, compliance officer(s) and internal auditor(s); and
- Persons charged or convicted of offences involving fraud, dishonesty or other similar offences are not employed by the financial institutions.

Chapter 5 – Wire Transfers

Article 29

Pursuant to Article 46 of the Law, financial institutions that engage in cross-border wire transfers should include accurate originator and recipient information on wire transfers and related messages and ensure that the information remains with the wire transfer or related messaged throughout the payment chain. Information accompanying all wire transfers should always contain:

Verified originator information as follows:

a) The full name of the originator;
b) The originator account number where such an account is used to process the transaction or a unique transaction reference, in the absence of an account, which permits traceability of the transaction.
c) The originator's address, or customer identification number, or date and place of birth;

Beneficiary information as follows:

a) The name of the recipient;
b) The recipient account number where such an account is used to process the transaction or a unique transaction

reference, in the absence of an account, which permits traceability of the transaction.

If the financial institutions are unable to comply with these requirements, it should not execute the wire transfers.

Article 30

Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, financial institutions may choose to not apply requirements of Article 29 above in respect of originator information, provided that they include the originator's account number or unique transaction reference number which permits traceability of the transaction, and the batch file contains required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country.

Ordering financial institutions shall ensure that non-routine wire transfers are not batched where this would increase the risk of money laundering or terrorism financing.

Article 31

For domestic wire transfers financial institutions are required to apply IBAN requirements as per the Instructions issued by the Central Bank of Oman.

Article 32

Ordering financial institutions should not execute cross-border wire transfers that do not include accurate and complete originator and beneficiary information. Ordering financial institutions shall maintain all originator and beneficiary information collected in accordance with the record keeping requirements of these Instructions.

Article 33

For cross-border wire transfers, financial institutions processing an intermediary element of the payment chain should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it, and should keep all wire transfer information including originator and beneficiary information in accordance with the record keeping requirements of these Instructions.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with related domestic wire transfer information, the intermediary financial institutions should keep a record, for at least ten years of all the information received from the ordering financial institutions or another intermediary financial institution.

Intermediary financial institutions should have effective risk-based procedures that are consistent with straight through processing for:

a) Identifying cross border wire transfers that lack required originator and/or beneficiary information;
b) Determining when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information and considering reporting to the Center; and
c) Taking appropriate follow-up action which may include restricting or terminating business relationships.

Article 34

Beneficiary financial institutions should take reasonable measures to identify cross border wire transfers that lack required originator or beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible. The beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with the record keeping requirements of these Instructions.

Beneficiary financial institutions should have effective risk-based procedures for:

a) Identifying cross border wire transfers that lack required originator and/or beneficiary information;
b) Determining when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information and considering reporting to the Center; and
c) Taking appropriate follow-up action which may include restricting or terminating business relationships.

Article 35

Financial institutions should have procedures in place to detect wire transfers with countries identified pursuant to Article 13(K) of the Law and to take appropriate action, as required by the Committee.

Chapter 6- Reporting Obligations and Provision of Information

Article 36

1) Pursuant to Article 47 of the Law, financial institutions, their managers, members of the board of directors, owners, authorized representatives, employees, agents, partners and professionals appointed to perform any tasks on their behalf should promptly notify the Center if they suspect or have reasonable grounds to suspect that funds are the proceeds of crime, or are related to terrorism financing. The notification should occur immediately 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 a predicate, money laundering or terrorism financing offense. Notifications should include all relevant information, document and records relating to the transaction, customer or account involved, and comply with the procedures and requirements set out by the

Center. Article 47 of the Law provides that there should be no penal, civil, or administrative liability for reporting persons when reporting according to the provisions of the Law.

2) Pursuant to Article 49 of the Law, reporting persons should 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. It is recognized that, as an operational necessity, such information may need to be exchanged between officers of the financial institution for the purposes of preparing and processing communications with the Center.

Article 37

Financial institutions should provide any relevant information or copies of documents or files, however stored, in response to any requests received from the Center and within the timeframe prescribed by or agreed with the Center.

Article 38

Financial Institutions should promptly report any cash transaction in an amount equal to or above to the Center, whether conducted as a single transaction or several transactions that appear to be

linked, in the format specified by the Center. Format and threshold for banks, money exchange establishments and finance leasing companies shall be advised separately later on.

Chapter 7 - Sanctions

Article 39

Without prejudice to any punishment stipulated for in the Law, a financial institution in violation of its obligations under the Law or these instructions shall be liable to one or more of the sanctions set forth in Article (52) of the Law.

Annex 1: Examples of indicators where ML/TF risks are considered high

Pursuant to Article 34(b) of the Law, financial institutions shall apply enhanced due diligence measures where they consider that the risk of money laundering or terrorism financing is higher. Indicators of high risk may include but are not limited to the following:

a) Customer risk factors:

- The business relationship is conducted in unusual circumstances.
- Non-resident customers.
- Legal persons or arrangements that are personal asset-management vehicles.
- Companies that have nominee shareholders or shares in bearer form.
- Businesses or activities that are cash-intensive or particularly susceptible to money laundering or terrorism financing.
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

- Business relationships and transactions conducted other than “face to face”.
- Business relationships conducted in or with countries as identified in (b) below.
- Politically exposed persons ("PEP").
- High net worth customers, or customers whose source of income or assets is unclear.

b) Country or geographic risk factors, having regard to Articles 41(b) and (d) of the Law:

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

c) Product, service, transaction or delivery channel risk factors:

- Private banking.
- Cash and other bearer or negotiable instruments.
- Accounts opened, business relationships or transactions conducted with customers that are not physically present for the purpose of identification.
- Payment received from unknown or un-associated third parties

Annex 2: Examples of enhanced due diligence measures for high risk customers

Pursuant to Article 36(a) of the Law, financial institutions must increase the degree and nature of ongoing monitoring in high-risk cases. Enhanced customer due diligence measures may include but are not limited to the following:

- To obtain additional information on the customer, beneficial owner, beneficiary and transaction.
- To establish and maintain a comprehensive risk profile on customers and transactions. The customer profile should be based upon sufficient knowledge of the customer and beneficial owner(s), the intended nature of the business relationship with the financial institutions, and on the source of funds and source of wealth of the customer.
- To update more regularly the information on customers and beneficial owners.
- To obtain information on the purpose of intended or performed transactions.
- To obtain the approval of senior management to commence or continue the business relationship.
- 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.

- To require the first payment to be carried out through an account in the customer's name with a financial institution subject to similar customer due diligence standards.
- To adopt other measures as may be prescribed by the Committee.