VENTURE CAPITAL BANK B.S.C. (C)

ANTI-MONEY LAUNDERING MANUAL

VENTURE
CAPITAL
BANK

TABLE OF CONTENTS

1. INTRODUCTION

1.1 NATURE AND PURPOSE OF THIS MANUAL

This Manual sets out Venture Capital Bank ("the Bank's") comprehensive policies and procedures for preventing money laundering and combating the financing of terrorism. The Manual covers the Anti-Money Laundering (AML)/Know Your Customer (KYC) policies required to conduct the Bank's business in compliance with guidelines provided by the Regulator. Detailed procedures are included on KYC and customer due diligence, internal and external Suspicious Transaction reporting (STR), staff training and record keeping.

The Manual aims to assist all members of management and staff to understand:

- The legal requirements and the different penalties for non-compliance;
- Requirements of the Bank pertaining to AML; and
- Method to recognize money laundering activities and the related actions required to be taken.

All members of the Bank's management and staff are expected to:

- Be aware of their personal legal obligations and the legal obligations of the Bank;
- Be aware of the Bank's policies and follow the Bank's procedures;
- Be alert for any suspicious financial activity; and
- Report on suspicious financial activity in line with internal procedures.

1.2 STRUCTURE OF THIS MANUAL

The AML policy and procedure Manual has been divided into following sections:

Money Laundering

This section defines money laundering, the process of money laundering and various stages involved in the process of money laundering.

The Bank's Policy

This section highlights Bank's policy with regards to regulatory AML compliance, customers' acceptance, customers' due diligence and responsibilities of the MLRO.

Customer Identification - General Principles

This section provides general principles for the verification of customers' identification, timing of verification and other KYC formalities.

Customer Identification – Exceptional Circumstances

This section provides principles for verification of customers' identification, timing of verification and other KYC formalities, in case of exceptional circumstances.

Ongoing Customer Due Diligence and Monitoring

This section highlights the Bank's policy for reviewing existing customer due diligence information on a regular basis.

Transactions through Correspondent Relationship

This section details the procedures that need to be carried out for correspondent banks and describes the KYC formalities and other requirements.

Introduced Business from Professional Intermediaries

This section includes the policies and procedures when the business is being referred by other banks or introducers.

Money Transfers

This section provides minimum requirements which should be complied with, in case of inward/outward fund transfers.

Monitoring Accounts for Suspicious Activity

This section defines various types of activities and transactions that should be monitored and reported.

Reporting Suspicions

This section outlines different stages of the Bank's suspicious transaction reporting procedure.

Combating the Financing of Terrorism

This section presents treatment of transactions, which have no apparent economic or visible lawful purpose.

Record Keeping

This section provides the document retention policy of the Bank as per the CBB regulations.

Education and Training

This section details the Bank's education and training policy for the existing and new staff members in context of AML.

Annual Compliance Report

This section discusses the scope of the review of the effectiveness of AML/CFT controls.

Acknowledgement

This section comprises an acknowledgement form that should be submitted by all concerned staff members to the Human Resource department. The acknowledgment form should be filed into the personnel files of all concerned staff. The MLRO should also receive a copy of the signed acknowledgement forms.

1.3 REVIEW AND APPROVAL

The Board of Directors (BoD) of the Bank has approved the AML policy and procedure Manual. Extracts of the minutes of the BoD meeting at which this Manual has been approved can be obtained from the Board Secretary.

The MLRO shall review the Manual at least once a year to ensure that it is in line with the changes in the Bank's product, operational procedures, and/or any other changes introduced by the CBB and other regulatory authorities that may have an impact on the processes described in the Manual. The amendments will be approved in writing by the BoD.

Revised copies and index pages will be immediately issued by the MLRO and a revised Manual will be sent to all Manual holders reporting such modifications.

2. MONEY LAUNDERING

Money Laundering is the process by which the direct or indirect benefit of crime is channelled through financial institutions to conceal the true origin and ownership of the proceeds of criminal activities. If successful, the money can lose its criminal identity and appear legitimate.

Generally, the process of money laundering comprises three stages, during which there may be numerous transactions that could alert a bank to the money laundering activity:

- **Placement:** the physical placement of illegally derived funds into the financial system, usually through a financial institution;
- **Layering:** the separation of the benefits of criminal activity from their source by creating layers of financial transactions designed to disguise the audit trail and provide anonymity; and
- **Integration:** the placement of funds back into the economy to give the appearance of a legitimate source.

The financing of terrorism is the financial support, in any form, of terrorism or those who encourage, plan or engage in terrorism. Those involved in terrorist financing transfer funds that may be legal or illicit in origin in such a way as to conceal their source and ultimate use, which is the support of terrorism.

The techniques used to launder money are essentially the same as those used in terrorist financing. If the source can be concealed, it remains available for future terrorist financing activity. Similarly, it is important for terrorists to conceal the use of funds so that the financing activity goes undetected.

The policies and procedures included in this Manual are designed to address the issue of financial crime, both in terms of money laundering and terrorist financing.

2.1 OBJECTIVES

From the perspective of the Bank, the prevention of money laundering has three objectives:

- **Ethical** – taking part in the fight against crime;
- **Professional** – ensuring that the Bank is not involved in recycling the proceeds of crime that could call into question its reputation, integrity and, if fraud is involved, its solvency; and
- **Legal** – complying with Bahrain legislation and regulations that impose a series of specific obligations on financial institutions and their employees.

These policies and procedures are intended to prevent the Bank's operations and activities from being used for unlawful purposes. To this end, it is imperative that the Bank accepts only those customers whose identity and source of wealth and funds can reasonably be established as legitimate.

2.2 DEFINITIONS

Anti-Money Laundering Unit (AMLU)

The AMLU is Bahrain's financial intelligence unit. It is a part of the Anti – Economic Crime Directorate (AECD) of the Ministry of Interior General Directorate of criminal investigation. It receives Suspicious Transaction Reports (STRs) filed by institutions covered by Decree Law 4/2001.

Authorized Money Transferor

Any bank or other licensee (such as money changers) specifically authorized to affect money transfers.

Customer

Any person seeking to form a business relationship or carry out a one-off transaction, with the Bank.

Customer Due Diligence Measures

Measures taken by the Bank to obtain information which accurately identifies a customer including:

- The financial circumstances of the customer; and
- The features of the transaction which the Bank has entered into with or for the customer.

Suspicious Transaction

Any transaction or deal which raises in the mind of a person involved, any concerns or indicators that such a transaction or deal may be related to money laundering or terrorist financing or any other unlawful activity.

3. THE BANK'S POLICY

3.1 GENERAL

It is the policy of the Bank to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the financing of terrorist or criminal activities. Therefore the Bank will not establish a relationship with, or conduct a transaction for, a customer;

- Whose funds appear to be the proceeds of or involved in an illegal activity;
- Whose identity or legitimacy cannot be satisfactorily established;
- Who fails to provide information which is necessary to comply with these policies;
- For whom there are inconsistencies or inaccuracies in the information provided which cannot be resolved after further investigation; or
- Who insists on opening or maintaining a secret, numbered account or an account in a false name.

The Bank's policy is intended to guard against the Bank's unintentional involvement as an intermediary in a process to conceal the true source of funds that were originally derived from criminal activity.

3.2 REGULATORY COMPLIANCE

It is the policy of the Bank to comply with the AML laws and regulations of the jurisdictions in which it undertakes business activities. The applicable AML laws and regulations include (but not limited to) the following:

- **Bahrain** – Legislative Decree No. 4 of the year 2001 with respect to Prohibition of and Combating Money Laundering; The Financial Crime module of the CBB Rulebook, first issued in July 2004 and revised quarterly;
- **United Nations ("U.N.") Security Council** – Anti-Terrorism resolution 1373 (2001) and Non-Cooperative Countries or Territories (NCCT) Notifications issued by the U.N. Security Council.

Bahrain, through its membership of the GCC is a member of MENA-FATF, which is a member of the Financial Action Task Force (FATF), an international body established in 1989 to develop and promote policies, both at national and international levels, to combat money laundering and terrorist financing.

The regulations implemented by the CBB in relation to combating money laundering and terrorist financing comply with the 40 Recommendations on Money Laundering and the 9 Special Recommendations on Terrorist Financing (known as the '40+9 recommendations') issued by the FATF. A list of FATF member countries is available on the website http://www.fatf-gafi.org

It is the policy of the Bank to apply the current Bahrain AML laws and regulations as the basis for customer identification, verification of the source of funds and the ongoing monitoring and reporting of suspicious transactions. In situations where the AML regulations of the other jurisdictions require additional customer due diligence procedures to be undertaken over and above the equivalent Bahrain regulations, such additional procedures will be performed in order to satisfy the requirements of all applicable jurisdictions.

The Bank also gives special attention to any dealings it may have with entities or persons domiciled in countries or territories which are:

- Identified by the FATF as being 'non-cooperative'; or
- Notified to the Bank from time to time by the CBB.

Whenever transactions with such parties have no apparent economic or visible lawful purpose, their background and purpose must be re-examined and the findings documented. If suspicions remain about the transaction, these must be reported to the relevant authorities in accordance with Section 11.3 of this Manual.

3.3 REGULATORY PENALTIES AS PER BAHRAIN LAW, DECREE 04/2001, ARTICLE 3

Any person committing, attempting or participating in a money laundering offence shall be liable to imprisonment for a period not exceeding seven years and a fine not exceeding BD One Million.

The punishment shall be imprisonment for a period of not less than five years and fine of not less than BD One Hundred Thousand in any of the following cases:

- The accused has committed the offence through an organised criminal gang;
- The accused has committed the offence by using his power or influence through an institution;
- The accused has committed the offence for the purpose of disguising the source of the proceeds which are derived from criminal activity to appear as of a lawful source.

Without prejudice to the rights of bona fide third parties a person convicted of the offence of money laundering shall in addition to the punishment prescribed, be liable to confiscation of property which is the subject matter of the offence, or any other property owned by him or by his spouse or his minor children, equivalent in value to the property which is subject matter of the offence.

The Court shall order the confiscation of such property on the extinction of the criminal proceedings due to the death of the accused provided that his heirs are unable to establish the lawful source thereof.

In cases where the offence of money laundering is committed by a corporate body and notwithstanding the liability of any natural person, the corporate body shall be liable to the punishment of a fine prescribed in this Law in addition to confiscation of the property which is the subject matter of the offence.

Any person who commits any of the offences related to money laundering shall be liable to imprisonment for a period not exceeding two years and/or a fine not exceeding BD Fifty Thousand or both.

Any person who contravenes the provisions of Regulations and Ministerial Regulations issued under this Law shall be liable to imprisonment for a period not exceeding three (3) months or a fine not exceeding BD Twenty Thousand or both.

Any of the accused who reports a money laundering offence to the Enforcement Unit before such offence is known to the Enforcement Unit shall be exempted from the punishment prescribed under this Law.

Where the accused reports the offence after it is known to the Enforcement Unit, his report shall lead to arrest or the other accused persons and attachment of property.

Without prejudice to any other penalty imposed by the CBB Law, the AML Law No. 4 or the Penal Code of the Kingdom of Bahrain, failure by the Bank to comply with the Financial Crime Module shall result in the levying by the CBB, without need of a court order and at the CBB's discretion, of a fine of up to BD 20,000.

3.4 GENERAL REQUIREMENTS

It is the policy of the Bank to maintain effective and systematic internal guidelines for establishing and verifying the identity of its customers.

It is the Bank's policy to;

- Collect certain minimum customer identification information from each customer;
- Verify the identity of each customer;
- Record customer identification information and the verification methods and results;
- Understand and obtain information on the purpose and intended nature of the business relationship.
- must conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

- Compare customer identification information with government-provided lists of suspected terrorists; and

- Respond to requests for information from the Bank's regulators and counterparties in a complete and timely manner, in accordance with local regulations.

3.5 UP-TO-DATE DOCUMENTATION

The Bank will take reasonable steps to ensure it receives and maintains up-to-date copies of customer identification documents as outlined under Section 6.

3.6 NEW CUSTOMERS

The Bank will not provide financial services to a new customer until it has obtained sufficient evidence to satisfactorily establish the customer's identity and source of funds.

3.7 EXISTING CUSTOMERS

The Bank will establish procedures to ensure the identification information held on existing customers is kept up-to-date. Where such information is found to be deficient, the Bank shall take steps to obtain such information as soon as possible, or shall terminate the relationship.

The Bank will review and update its customer due diligence at least once every three years for its existing customers. Upon performing such reviews, if copies of identification documents such as the C.P.R. or passport are found to be more than 12 months out-of-date, the Bank shall take steps to obtain new copies as soon as reasonably possible.

3.8 CUSTOMER ACCEPTANCE

In order to establish a relationship or conduct a significant transaction with a customer, the Placement Officer must complete a Know Your Customer form (KYC form) which contains all customer information. The completion of the KYC form is mandatory for Placement Officers who are responsible for enrolling new customers and should be completed by them in a comprehensive and accurate manner. The KYC form and the information therein assists the Bank to properly identify its customers and also provides the Bank with relevant financial and background information for each customer. Where necessary or appropriate, such information should be confirmed by independent verification.

The nature, amount and quality of information available from customers can and will vary depending upon, among other factors, the type of customer, the nature and extent of the relationship, the size and type of the transaction, and whether any suspicious indicators are present. Notwithstanding the aforementioned, the following shall be undertaken for each new customer relationship:

New Customer / Existing Customer

The following are the procedures to be followed when confirming that the prospective / existing customer is not appearing on a list of prohibited individuals and entities and whether prospective customer is to be categorized as a PEP or not:

- Using World-Check online service, the Placement Officer should confirm that the prospective customer does not appear on a list of prohibited individuals and entities issued by the United Nations, European Union or the United States Treasury Department Office of Foreign Assets Control ("OFAC"). Confirmation of the World-Check search is to be appended to the prospective customer's KYC form.

- An assessment as to whether or not the prospective customer should categorized as a PEP by applying the definition set forth in Section 5.1. Should the prospective customer be designated as a PEP, the independent Reviewing Officer and/or the Placement Officer shall undertake enhanced due diligence procedures by completing the prescribed PEP Enhanced Due Diligence checklist.

If at anytime doubts exist about the legitimacy of a customer or transaction, the Bank's employees are expected to exercise good judgment to make appropriate further inquiries of the customer, and if appropriate, notify the MLRO by filling an internal STR Form.

3.9 MONEY LAUNDERING REPORTING OFFICER (MLRO)

The Bank will appoint an MLRO and a Deputy MLRO, who will act in the absence of the MLRO. The MLRO is responsible for overseeing all AML activity within the Bank and must be approved by the CBB and be resident in Bahrain. The Deputy MLRO must also be a resident of Bahrain unless otherwise agreed with the CBB.

The position of MLRO must not be combined with functions that create potential conflicts of interest, such as internal auditor or business line head. The position of MLRO may not be outsourced either.

If the position of MLRO or Deputy MLRO falls vacant, the Bank must appoint a permanent replacement (after obtaining CBB approval), within 120 calendar days of the vacancy occurring. Pending the appointment of a permanent replacement, the Bank must make immediate interim arrangements (including the appointment of an acting MLRO or Deputy MLRO) to ensure the continuity in the function's performance. These interim arrangements must be approved by the CBB.

The MLRO will have unrestricted access to all transaction information relating to financial services provided by the Bank to a customer.

The MLRO is responsible for:

- Establishing and maintaining the AML/combating the financing of terrorism ('CFT') policies and procedures;

- Ensuring that the Bank complies with the applicable AML law;

- Ensuring the day-to-day compliance with the Bank's own internal AML/CFT policies and procedures;

- Acting as the Bank's main point of contact in respect of handling internal suspicious transaction reports from the Bank's staff and as the main contact for the Financial Intelligence Unit, the CBB and other concerned bodies regarding AML/CFT;
- Making external suspicious transactions reports to the Anti-Money Laundering Unit and Compliance Unit;
- Taking reasonable steps to establish and maintain adequate arrangements for staff awareness and training on AML/CFT matters;
- Producing annual reports on the effectiveness of the Bank's AML/CFT controls for consideration by senior management;
- On-going monitoring of what may, in his opinion, constitute high-risk customer accounts;
- Maintaining all necessary CDD, transactions, STR and staff training records for the required periods; and
- Making external reports to the Anti-Money Laundering Unit of the Ministry of Interior and the CBB.

3.10 TREATMENT OF EXISTING BUSINESS RELATIONSHIPS

It is a widely recognized tactic of money launderers to establish seemingly legitimate and normally run accounts, which are then used to launder money at a later date. Accordingly, the MLRO and Placement Officer will be responsible for ensuring that the identification information on existing customers meets the identification requirements set out in this Manual.

4. CUSTOMER IDENTIFICATION – GENERAL PRINCIPLES

4.1 THE NEED TO VERIFY IDENTITY

For each type of customer, documentation will be obtained and sufficient information will be gathered for the Bank to ensure that:

- Verification of new customer identity, address, business and expected level of transactions have been understood;
- The new customer has understood and accepted the Bank's terms and conditions; and
- The customers and their business are legitimate and the Bank is not at risk of financial loss or reputational damage.

The customer due diligence measures, outlined below, will be required when:

- Establishing business relations with a new or existing customer;
- A new signatory or beneficiary to an existing account or business relationship is introduced;
- A significant transaction with a customer takes place;
- There is a material change in the way that a business relationship functions;
- Customer documentation standards change substantially;
- The Bank has doubts about the veracity or adequacy of previously obtained customer due diligence data;
- Where an unusual transaction takes place;
- When a wire transfer takes place irrespective of the amount; or
- When there is a suspicion of money laundering or terrorist financing.

4.2 TIMING OF VERIFICATION – Comapnies under Formation or New Arrivals

The business relationship with a customer must not commence without the prior completion of customer due diligence measures. However, verification of identity may be completed after the receipt of funds, in the case of: Bahrain Companies under formation which are being registered with the Ministry of Industry and Commerce, or newly arrived persons in Bahrain who are taking up employment or residence, or where there is no face-to-face business or where the customer provides the customer due diligence documents subsequent to face-to-face contact. However, no disbursements of funds may take place until the customer due diligence measures has been completed within a reasonable timeframe.

4.3 CUSTOMER DUE DILIGENCE EXCEPTIONS

Exceptions to the standard customer due diligence procedures required by these policies and procedures must be approved in writing, recording the reasons for exceptions by the MLRO.

If a customer does not provide all the information required for completion of KYC form within forty five days from the receipt of funds for the purpose of participation in an investment, the Bank in consultation with the Placement Officer, and the MLRO shall terminate its business with that customer by closing the customer's account and return the funds to the account from which they were received. If there is any suspicion surrounding the non-provision of information by the customer, an internal STR must be submitted to the MLRO.

In addition, the customer due diligence evidence that gives rise to the said exception(s) is to be obtained as soon as practicable after the relationship has arisen. The customer's funds are not to be paid-out or transferred from a Bank controlled account before all customer due diligence evidence has been obtained in accordance with these policies and procedures unless approved otherwise by the MLRO.

While the initial customer review is critical for implementing this policy, continued customer monitoring and review is equally important. All appropriate employees are expected to dutifully maintain and update customer identification records when there are material changes.

4.4 CUSTOMER DUE DILIGENCE – NATURAL PERSONS

The potential relationship of the customer with the Bank must be clearly established. Before providing financial services of any kind to an individual (i.e. a natural person), the individual must complete the standard KYC form and the Placement Officer must ensure that the KYC form is complete and the following information recorded:

- Full name and any other names used;
- Full physical address (a P.O Box number is not acceptable);
- Date and place of birth;
- Nationality;
- Passport number;
- CPR (for Bahrain residents) or Iqama number (for GCC residents);
- Telephone number, fax number and e-mail address;
- Occupation or public position held;
- Employer's name and address;
- Type of account and nature and level of business relationship with the Bank;
- Signature of the Placement Officer; and
- Source of funds statement.

By signing the KYC form the Placement Officer acknowledges that client funds have been generated through legitimate business activities that he or she is not aware of any reasons why the client should be prohibited from dealing with the Bank and that the Placement Officer recommends acceptance of this account.

4.5 DOCUMENTATION FOR EVIDENCE OF IDENTITY – NATURAL PERSONS

The Placement Officer must verify the information specified in section 4.4 "Full name", "CPR (for Bahrain residents) or Iqama number (for GCC residents)" by the following method below; at least one of the copies of the identification documents mentioned in the first two points below must include a clear photograph of the customer:

- Confirmation of the date of birth and legal name, by taking a copy of a current valid official original identification document (e.g. birth certificate, passport or Iqama);
- Confirmation of the permanent address by taking a copy of a recent utility bill, bank statement or similar statement from another licensee or financial institution, or some form of official correspondence or official documentation card, such as CPR, from a public/governmental authority, or a tenancy agreement or record of home visit by an official of the Bank; and
- Where appropriate, direct contact with the customer by phone, letter or e-mail to confirm relevant information, such as residential address information.

4.6 CUSTOMER DUE DILIGENCE – LEGAL PERSONS

Before providing financial services of any kind to a legal entity such as a partnership, trust or company, the Placement Officer will be responsible for completing the standard KYC form and ensuring that the following information has been obtained:

- Entity name;
- Registration number;
- Legal form;
- Registered address (and trading address where applicable);
- Type of business activity;
- Date and place of incorporation or establishment;
- Type of account and nature and level of business relationship with the Bank;
- Telephone, fax, and e-mail address;
- Regulatory or listing body;
- Name of external auditor; and

- Information concerning the source of wealth / income.

By signing the KYC form the Placement Officer acknowledges that client funds have been generated through legitimate business activities that he or she is not aware of any reasons why the client should be prohibited from dealing with the Bank and that the Placement Officer recommends acceptance of this account.

4.7 DOCUMENTATION FOR EVIDENCE OF IDENTITY – LEGAL PERSONS

The details given in section 4.5 "Entity name" and "Registered Address" must be verified by obtaining certified copies of the following documents:

Public Companies

- Certificate of Incorporation and/or Certificate of Commercial Registration;
- Memorandum and Articles of Association;
- Board resolution seeking banking services;
- Copies of latest financial reports and accounts, audited where possible;
- Names, nationality and date of birth of the directors and officers; and
- List of authorized signatories and identification documents of the authorized signatories (as per section 4.4 above).

Private or Unlisted Companies

- Certificate of Incorporation and/or Certificate of Commercial Registration;
- Memorandum and Articles of Association;
- Board resolution seeking banking services;
- Copies of latest financial reports and accounts audited where possible;
- Names, nationality, country of residence and date of birth of the directors and officers;
- Identification documents of the directors and officers (as per section 4.4 above);
- Obtain and verify the identity of shareholders holding 20% or more of the issued capital;
- List of authorized signatories and identification documents of the authorized signatories (as per section 4.4 above); and

- Enquire as to the structure of the legal entity or trust sufficient to determine and verify the identity of the ultimate beneficial owner of the funds, the ultimate provider of funds (if different), and ultimate controller of the funds (if different).

For the purpose of obtaining a certified copy of the commercial registration as stated above, this requirement can be satisfied by obtaining a commercial registration abstract printed directly from the Ministry of Industry, Commerce and Tourism's website, through "SIJILAT Commercial Registration Portal".

Partnerships

- Partnership agreement;
- Partnership registration documents;
- Names, nationality, country of residence and date of birth of the partners;
- Identification documents of the partners (as per section 4.4 above); and
- List of authorized signatories and identification documents of the authorized signatories to operate the account (as per section 4.4 above).
- Latest available financial statement.

Trusts

- Trust deed;
- Trust registration documents; and
- Identification documents of the settlor, the trustee and the beneficiaries (as per section 4.4 above).

The Bank must also enquire as to the structure of the legal entity or trust, sufficient to determine and verify the identity of the ultimate beneficial owner of the funds, the ultimate provider of the funds and the ultimate controller of the funds.

In the case of a Trust, the Placement Officer, in addition to verifying identity of the trustees and signatories, must also:

- Make appropriate enquiry as to the general nature of the trust (e.g. family trust, pension trust) and the source of funds;
- Obtain identification evidence for the settlor(s), i.e. the person(s) whose property was settled on trust; and
- In the case of a nominee relationship, obtain identification evidence for the beneficial owner(s) if different to the settlor(s).

Where a legal entity authorizes another person to perform an activity on its behalf, the Placement Officer must sight the original board resolution and file a certified copy for record.

The Bank must also ascertain, to the reasonable extent possible, whether the legal entity has been or is in the process of being wound up, dissolved, struck off or terminated.

In addition, the Placement Officer must also carry out one of the following for all new corporate customers:

- A visit to the entity; or
- Contact the entity by phone, mail or e-mail.

4.8 Non-Resident Account

Accounts opened for GCC nationals, not resident in Bahrain, are subject to the customer due diligence measures outlined in CBB rulebook Volume two Sections FC-1.2 (face-to-face) or FC-1.4 (non face-to-face). Where a customer is resident outside of the GCC, the guidance provided in Section FC-1.3 should be referred to.

Where a non-resident account is opened, the customer must be informed by the bank of any services which may be restricted or otherwise limited, as a result of their non-resident status.

4.9 VERIFICATION OF IDENTITY OF ULTIMATE BENEFICIARY

A signed statement must be obtained from all new customers confirming whether or not the customer is acting on their own behalf or not. This undertaking must be obtained as part of the KYC form.

The identity of the customer and, where applicable, the party or parties on whose behalf the customer is acting must be established and verified. Where a customer is acting on behalf of third parties, the Placement Officer must obtain a signed statement from the beneficial owner that he/they are the ultimate beneficiary(ies) of the account/facility and have given authority to the customer to act on their behalf.

4.10 CERTIFYING AUTHORITIES

Any documents used for the purpose of identification verification should be original documents. Where the Bank makes a copy of an original document, the copy should be dated, signed and marked “original sighted” by the concerned Bank official.

Any identity documents which are not obtained directly by an authorized official of the Bank in original form (e.g. due to the customer sending a copy by post following an initial meeting) must be certified and signed by one of the following from a GCC or FATF member state:

- A registered lawyer;
- A registered notary;
- A chartered/certified accountant;
- A government ministry official;
- An official of an embassy or consulate; or
- An official of another licensee of the CBB.

The individual above making the certification should give clear contact details (e.g. a business card or company stamp). The Bank will verify the identity of the person providing the certification by checking the membership of a professional organization (e.g. for a lawyer or an accountant), or through databases or websites, or directly by phone or email contact.

4.11 REPORTING SUSPICIOUS CIRCUMSTANCES

If there are any suspicious circumstances surrounding the opening or operation of any account, the matter must be reported immediately to the MLRO using the Suspicious Transaction Internal Report Form.

4.12 CUSTOMERS WHO REFUSE TO PROVIDE INFORMATION

If a potential or existing customer either refuses to provide the information when requested, or appears to have intentionally provided misleading information, the Bank must not open a new account and it should freeze any funds received and file a suspicious transaction report; or to terminate the relationship; or return the funds to the customer in the same method as received., In either case, the MLRO will be notified so that he/she can determine whether to report the matter to the Head of the Compliance Unit at the CBB.

4.13 SERVICES TO MINORS / PERSONS LACKING FULL LEGAL CAPACITY

Where financial services are provided to a minor or other person lacking full legal capacity, the normal identification procedures as set out must be followed. In the case of minors, the Bank must additionally verify the identity of the parent(s) or legal guardian(s). Where a third party on behalf of a person lacking full legal capacity wishes to open an account, the Bank must establish the identity of that third party as well as the intended account holder.

4.14 ANONYMOUS AND NOMINEE ACCOUNTS

Anonymous accounts or accounts in fictitious names must not be established or maintained. In addition, nominee accounts, which are controlled by or held for the benefit of another person, whose identity has not been disclosed, must not be established or maintained.

4.15 SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES

Simplified due diligence may be applied in the following circumstances:

- The customer is the Central Bank of Bahrain ('CBB'), the Bahrain Stock Exchange ('BSE') or a licensee of the CBB;
- The customer is a Ministry of a Gulf Cooperation Council ('GCC') or Financial Action Task Force ('FATF') member state government, a company in which a GCC or FATF government is a majority shareholder, or a company established by decree in the GCC;
- The customer is a company listed on a GCC or FATF member state stock exchange (where the FATF state stock exchange has equivalent disclosure standards to those of the BSE);
- The customer is a financial institution whose entire operations are subject to AML/CFT requirements consistent with the FATF Recommendations / Special Recommendations and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements;

- The customer is a financial institution which is a subsidiary of a financial institution located in a FATF or GCC member state, and the AML/CFT requirements applied to its parent also apply to the subsidiary;

- The customer is a borrower in a syndicated transaction where the agent bank is a financial institution whose entire operations are subject to AML/CFT requirements consistent with the FATF Recommendations / Special Recommendations and it is supervised by a financial services supervisor in a FATF or GCC member state for compliance with those requirements; or

- The transaction is unusual in nature.

For customers falling under the above categories, the customer due diligence information must be obtained, however, the verification and certification requirements may be dispensed with.

In respect of the above, the Bank shall obtain the customer's full name. The identity of all signatories need not be verified if the entity issues official authorized signature lists which the Bank receives. In all other cases full verification of the identity of the signatories must take place (as per section 4.4).

For financial institutions covered above, the Bank will obtain documentary evidence such as list of licensees in the concerned country issued by the appropriate regulatory authority (e.g., from its website) as well as evidence of the AML/CFT requirements to support the case for simplified due diligence.

The Bank will use authenticated SWIFT messages as a basis for confirmation of the identity of a financial institution where it is dealing as principal. For subsidiaries, the Bank will obtain a written statement from the parent institution of the concerned subsidiary confirming that the subsidiary falls under the same AML/CFT provisions as the parent.

However, the MLRO will satisfy himself appropriately that the customer falls under the aforementioned categories and will record the basis upon which he/she is so satisfied.

4.16 SUSPICOUS ACCOUNTS WATCH LIST

The Bank will adhere to CBB requests and recommendations in dealings with persons whose names are contained on its Suspicious Accounts Watch List.

4.17 SHELL BANKS

The Bank will not establish any business relationship with banks which have no physical presence or whose management is not present in the jurisdiction in which they are licensed, otherwise known as 'shell banks'. In addition, the Bank will not establish relationships with any banks that are known to have relations with shell banks.

The Bank must make a suspicious transaction report to the Anti-Money Laundering Unit and the Compliance Unit if they are approached by a shell bank or an institution they suspect of being a shell bank.

4.18 RISK SENSITIVE CUSTOMER DUE DILIGENCE

Customer due diligence must be performed based on the categorization of customers according to perceived risk. For example:

High Risk Entities – These customers will include;

- Firms with silent partners;

- Politically exposed persons;
- Non face to face customers;
- Person with doubtful reputation as per public information available;
- Non-Resident Customers; and
- High Net Worth Individuals categorized on the basis of the customer's background, nature and location of activity, country of origin, sources of funds and customer profile.

Low Risk Entities – Those who are not defined as High Risk Entities above.

The Placement Officer should perform enhanced due diligence on customers identified as having a "higher risk profile" after initial assessment. Determining whether a customer has a "higher risk profile" requires the exercise of judgment by the Bank's officials. The following list is indicative of the type of customers that may fall within this category:

- Reluctance to provide information or providing minimal information;
- Non face-to-face business and the use of new technologies, such as the internet or telephone banking;
- Pooled funds;
- Correspondent banking relationships;
- The use of unusual or suspicious identification that cannot be readily verified;
- Non-governmental organizations (e.g. charitable organizations and religious, sporting, social, cooperative and professional societies); or
- Offshore corporations, bearer share corporations and banks located in tax and/or secrecy havens and jurisdictions designated as non-cooperative in the fight against money laundering.

Enhanced due diligence must be performed on such customers identified as having a higher risk profile.

Full details of the Bank's enhanced customer due diligence policies and procedures can be found in section 5.

5. CUSTOMER IDENTIFICATION – ENHANCED DUE DILIGENCE

Enhanced customer due diligence must be performed on those customers identified as having a higher risk profile, and additional inquiries made or information obtained in respect of those customers.

The additional information will include documents (either in hard copy or electronic format) relating to the following:

- Evidence of a person's permanent address through the use of a credit reference agency search or through independent verification by home visit;
- A personal reference (e.g. by an existing customer of the Bank);
- Reference check from another financial institution regarding the customer;
- Documentation outlining the customer's source of wealth;
- Documentation outlining the customer's source of income; and
- Independent verification of employment, or public position held.

5.1 POLITICALLY EXPOSED PERSONS ("PEPS")

Persons commonly referred to as "politically exposed persons" (PEPs) are individuals who have been entrusted with prominent public functions by an international organisation and include heads of state, ministers, influential public officials, judges and military commanders. PEPs should be identified at the time of opening the account relationship and on a periodic basis. Publicly available information should be used to establish whether a customer is PEP. The approval of the MLRO must be obtained for establishing business relationships with such customers.

Where an existing customer is a PEP, enhanced monitoring and customer due diligence measures should be carried out which include:

- Analysis of complex financial structures, including trusts, foundations or international business corporations;
- A written record in the customer file to establish that reasonable measures have been taken to establish both the source of wealth and source of funds;
- Development of a profile of anticipated account activity to be used in ongoing account monitoring;
- Approval of senior management for allowing the customer relationship to continue; and
- Ongoing account monitoring of the PEPs account should be performed by the relevant Placement Officer on a regular basis.
- The requirements for all types of PEP must also apply to family or close associates of such PEPs.

5.2 CHARITIES, CLUBS AND OTHER SOCIETIES

Accounts must not be opened for charitable funds and religious, sporting, social, cooperative and professional societies until an original certificate authenticated by the relevant Ministry confirming their identities and authorizing them to open an account has been obtained. Further, for clubs and societies registered with the Ministry of Youth and Sport Affairs, the bank must contact the Ministry to clarify whether the account may be opened in accordance to their rules. If the sport association registered with Bahrain Olympic Committee (BOC), the bank must contact (BOC) to clarify whether the account may be opened in accordance to their rules.

All transfers of BD 3,000 or above from accounts held by charities registered in Bahrain must be reported to the CBB's Compliance Directorate giving details of the amount transferred, account name, number and bank details.

The Bank may not accept or process any incoming or outgoing wire transfers from or to any foreign country on behalf of charity and non-profit organizations licensed by the Ministry of Social Development until an official letter by the Ministry of Social Development authorizing the receipt or remittance of the funds has been obtained by the concerned bank.

Pursuant to Article (20) of the Consolidated Financial Regulations for Sports Clubs issued in 2005, the bank must not change or open additional bank accounts for Clubs and Youth Centres without obtaining the prior approval of the Ministry of Youth and Sport Affairs.

5.3 NON FACE-TO-FACE BUSINESS AND NEW TECHNOLOGIES

Where no face-to-face contact takes place, the Bank must take additional measures in order to mitigate the potentially higher risk associated with such business. In particular, the Bank must take measures:

- To ensure that the customer is the person they claim to be; and
- To ensure that the address provided is genuinely the customers.

The following checks can assist the Bank verify the authenticity of the applicant:

- Telephone contact with the applicant on an independently verified home or business number;
- With the applicant's consent, contact with their employer to confirm employment; or
- Evidence of salary details appearing on bank statements.

Financial services provided via post, telephone or internet pose greater challenges for customer identification and AML/CFT purposes. Any electronic or internet banking initiatives should incorporate procedures to enable the Bank to highlight and report unusual transactions.

The bank must identify and assess the money laundering or terrorist financing risks that may arise in relation to:
(a) The development of new products and new business practices, including new delivery mechanisms; and
(b) The use of new or developing technologies for both new and pre-existing products. To do so, such a risk assessment must take place prior to the launch of the new products, business practices or the use of new or developing technologies. The bank must take appropriate measures to manage and mitigate those risks.

5.4 POOLED FUNDS

Where the Bank receives pooled funds from professional intermediaries, such as investment and pension fund managers, stockbrokers and lawyers or authorized money transferors, the Placement Officer must verify the identity of the intermediary.

Where the funds are not co-mingled (i.e. there are individual sub-accounts attributable to each beneficiary), the Placement Officer must also verify the identity of each beneficial owner.

If funds are co-mingled, the Placement Officer must make reasonable efforts to look beyond the intermediary and determine the identity of the beneficial owners, particularly where funds are banked and then transferred onward to other financial institutions.

If, however, the intermediary is subject to regulations equivalent to those applied by the CBB, the Placement Officer need to confirm only that customer due diligence process is in line with the CBB requirements.

If the intermediary is based in a foreign jurisdiction, the Bank must obtain documentary evidence that they are subject to AML and CFT requirements consistent with the FATF 40+9 Recommendations and that the intermediary is supervised for compliance with those regulations. The Bank must also obtain evidence that the intermediary has identified the underlying beneficiaries and that it has systems and controls in place to allocate assets to individual beneficiaries.

6. ONGOING CUSTOMER DUE DILIGENCE AND MONITORING

While the initial customer review is critical for implementing this policy, continued customer monitoring and review is equally important. Employees are expected to dutifully maintain and update customer identification records when there are material changes.

The Bank will review the customer due diligence information on existing customers at least every three years. When an existing customer closes one account and opens another, the Bank will review the customer identity information and update its records accordingly. In the case of information more than 12 months out of date or missing data, this will be obtained and re-verified with the customer.

7. TRANSACTIONS THROUGH CORRESPONDENT RELATIONSHIPS

The Head of Operations in conjunction with the MLRO must ensure that normal customer due diligence measures are carried out on respondent banks and that the Bank has sufficient information about the respondent to fully understand its business.

The Head of Operations collects the following information before the Bank enters into any correspondent banking relationship:

- Information on the respondent's ownership structure and management;
- Major business activities of the respondent and its location as well as the location of its parent (where applicable);
- Where the customers of the respondent bank are located;
- Money laundering prevention and detection controls;
- Purpose of the account;
- The extent to which the respondent performs ongoing due diligence on customers and the condition of regulation and supervision in the respondent's country;
- Confirmation that the respondent bank has verified the identity of any third party entities that will have direct access to the correspondent banking services without reference to the respondent bank (e.g. in the case of "payable through" accounts);
- Confirmation that the respondent bank is able to provide relevant customer identification data on request to the correspondent bank; and
- Investigations into whether the respondent bank has been subject to a money laundering or terrorist financing investigation.

Further, the Head of Operations must ensure that, prior to opening a correspondent banking relationship:

- There is a signed document approved by the CEO or his delegate, outlining the respective responsibilities of each institution;
- The establishment of the correspondent banking relationship has the approval of the senior management; and
- A correspondent relationship has not been entered into or maintained with a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group (i.e. shell bank).

8. INTRODUCED BUSINESS FROM PROFESSIONAL INTERMEDIARIES

There may be circumstances where obtaining customer due diligence evidence is an unnecessary duplication of effort. In such circumstances, the Bank may decide to rely on the procedures undertaken by other banks or introducers when the business is being referred.

Reliance placed on the due diligence undertaken by an introducer, however, does not remove the ultimate responsibility of the Bank to know its customers and their business. The Bank may, therefore, rely on the performance of customer due diligence in whole or in part by another financial institution (including an affiliate) or intermediaries. This applies to any customer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings or other financial transactions.

Introducers may be relied upon in the following circumstances:

- The customer due diligence measures applied by the introducer are consistent with those required by the FATF 40+9 Recommendations;
- A formal agreement is in place defining the respective roles of the Bank and the introducer in relation to customer due diligence procedures and the agreement specifies that the customer due diligence measures of the introducer will comply with the FATF 40+9 Recommendations;
- The introducer is able to provide all relevant data pertaining to the customer's identity, the beneficial owner of the funds and, where applicable, the party or parties on whose behalf the customer is acting;
- The introducer has confirmed that the Bank will be allowed to verify the customer due diligence measures undertaken by the introducer at any stage; and
- Written confirmation is provided by the introducer confirming that all customer due diligence measures required by the FATF 40+9 Recommendations have been followed and the customer's identity established and verified. In addition, the confirmation must state that any identification documents or other customer due diligence material can be accessed by the Bank and that these documents will be kept for at least five years after the business relationship has ended.

In the event that the Bank is not satisfied that the introducer has taken adequate and appropriate steps to identify the customer, the Bank shall perform the customer due diligence measures itself or not commence or continue the relationship.

The Bank shall also perform periodic reviews to ensure that any introducer it relies upon continues to comply with appropriate customer due diligence measures.

9. MONEY TRANSFERS

9.1 INCOMING WIRE TRANSFERS

The Bank's Operations department will carefully scrutinize incoming wire transfers that do not include complete originator information, i.e.

- The name of the payer;
- The address of the payer; and
- The account number or unique customer identification number of the payer.

Should the Bank's Operations be unable to obtain promptly any missing Originator Information from the remitting institution, then details of the wire transfer shall be summarized and forwarded immediately to the MLRO for further action as a possible suspicious transaction, which may be reported to the CBB.

In case of inward transfers the Bank will:

- Maintain records of all originator information received with an inward transfer;
- Carefully scrutinize inward transfers, which do not contain originator information. If originator information is not present the funds will be returned to the sending institution in consultation with the Placement Officer and MLRO and these transactions will be deemed to be suspicious and should be passed on to the MLRO for determination as to possible filing of an STR unless:
  - The sending institution is able to provide the information within two business days; and
  - The sending institution and the Bank are acting as principals.

9.2 OUTGOING WIRE TRANSFERS

The Bank's Operations department will ensure that all outgoing wire transfers include details of originator information, i.e;

- The name of the payer;
- The address of the payer; and
- The account number or unique customer identification number of the payer.

When the Bank transfers funds using an Authorized Money Transfer to a customer or a person or organization in another country, records must be maintained of;

- The identity of the customer(s); and
- The exact amount transferred for each customer.

In addition, the Bank will return any money transferred inadvertently, back to the same account from which it was transferred in.

The Bank will not transfer funds for customers to a person or organization in another country by any means other than through an Authorized Money Transferor.

9.3 Cross-Border Wire Transfer

- The Bank's Operations department will ensure that all wire transfers must always contain:The name of the originator
- The originator account number or IBAN where such an account is used to process the transaction.
- The originator's address, or national identity number, or customer identification number, or date and place of birth
- The name of the beneficiary; and
- The beneficiary account number where such an account is used to process the transaction.

9.4 Domestic wire transfers

Information accompanying domestic wire transfers must also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and the CBB by other means. In this latter case, the originating financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.

9.5 Responsibilities of Originating, Intermediary and Beneficiary Banks

- Originating Bank

The originating bank must ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information, and must maintain all originator and beneficiary information collected in accordance with CBB rulebook paragraph FC-7.1.1. The bank must not execute the wire transfer if it does not comply with the abovementioned requirements.

- Intermediary Bank

For cross-border wire transfers, banks processing an intermediary element of such chains of wire transfers must ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept, for at least five

years, by the receiving intermediary bank of all the information received from the originating bank or another intermediary bank.

An intermediary bank must take reasonable measures to identify cross-border wire transfers that lack required originator information or required beneficiary information. Such measures must be consistent with straight-through processing.

An intermediary bank must have effective risk-based policies and procedures for determining:

- When to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
- The appropriate follow-up action.

- Beneficiary Bank

A beneficiary bank must take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.

For wire transfers, a beneficiary bank must verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with CBB rulebook Paragraph FC-7.1.1.

A beneficiary bank must have effective risk-based policies and procedures for determining:

- When to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and
- The appropriate follow-up action.

9.6 REMITTANCES ON BEHALF OF MONEY or Value Transfer Service (MVTS) Providers

When an Authorized Money or Value Transfer Service Providers is used to affect the transfer of funds for a customer to a person or organization in another country, the Bank must, in respect of the amount transferred, maintain records of:

- The identity of the customer(s); and
- The exact amount transferred for each such customer (particularly where a single transfer is affected for more than one customer).

The Bank will ensure that this information is readily available for inspection immediately upon the CBB's request.

In the case of an authorised MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the authorised MVTS provider:

- Must take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

- Must file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.

9.7 MONEY TRANSFERS BY UNAUTHORISED PERSONS

The Bank will not transfer funds for customers to a person or organization in another country by any means other than through an Authorized Money Transferor.

10. MONITORING ACCOUNTS FOR SUSPICIOUS ACTIVITY

Where a transaction is inconsistent in amount, origin, destination or type with a customer's known legitimate business or personal activities, the transaction must be considered unusual and the employee put on alert.

Activities that should put the employee on alert may be recognizable as falling into one or more of the following categories. This list is not meant to be exhaustive:

- Customer uses the Bank for a single transaction or very short period (eg Pass-through or "in and out" transactions);
- Transactions with entities which are not reasonably believed to have comprehensive customer due diligence and AML policies;
- Transactions with entities which are incorporated in or have their primary place of business in countries which have inadequate AML laws (specifically, countries that are not members of, or not affiliated with, the Financial Action Task Force);
- Business is out of line with the customer's preadvised or established pattern of business – volume, frequency, commodity, countries or profitability;
- Any unusual transaction in the course of some usual financial activity;
- Any unusually linked transactions;
- Any unusual employment of an intermediary in the course of some usual transaction or financial activity;
- Any unusual method of settlement;
- Transactions which yields an apparent profit (or loss) which is unusually high;
- The wide use of offshore accounts, companies or structures in circumstances where the customer's needs do not require such economic or legal requirements;
- Any unusual or disadvantageous early redemption of an investment product; and
- Any unwillingness by the customer to provide the information requested.

Where an employee conducts enquiries and obtains what he/she considers to be a satisfactory explanation of the unusual activity, he/she may conclude that there are no grounds for suspicion, and therefore take no further action.

10.1 RISK MANAGEMENT PROCEDURES AND ONGOING TRANSACTIONS MONITORING

- The Bank will develop and maintain a risk-based system taking into account the number of its customers, transactions and complexity of its business.

- As per the CBB, in the absence of risk-based monitoring system all transaction above BD 6,000 must be viewed as significant and be captured in daily transaction report, however due to the fact that the Bank's products/investments have a minimum participation/subscription limit of US$ 100,000 and the fact that the Bank are not engaged in to the money transfer businesses, the daily transaction report captured unusual transactions to be monitored by the MLRO or a relevant delegated Bank employee.

11. REPORTING SUSPICIONS

11.1 OVERVIEW

All reports of suspicious activity must be sent directly to the MLRO, and only the MLRO has the authority to determine whether a disclosure to the respective Reporting Authorities, in accordance with these policies and guidelines, is appropriate. There are four stages to the Bank's suspicious transaction reporting procedure:

- It is the duty of every member of management and staff to report any suspicious transactions to the MLRO;
- All internal Suspicious Transaction Reports must reach the MLRO and must not be blocked;
- The MLRO will investigate the report and will decide on the basis of all available information and additional enquiries whether or not the transaction or instruction remains suspicious or whether there is some additional information that removes the suspicion; and
- If the MLRO considers the suspicion to be justified, he will prepare a report for the Anti-Money Laundering Unit and the CBB using the Suspicious Transaction Report Form – MLRO. The Internal Report Form will remain on file within the Bank and will not be passed to the Anti-Money Laundering Unit and the CBB. The name of the individual member of staff who made the report will not be revealed.

11.2 INTERNAL REPORTING – RESPONDING TO RED FLAGS AND SUSPICIOUS ACTIVITY

The Bank must implement procedures to ensure that staff who handle customer business or are managerially responsible for such staff make a report promptly to the MLRO if they know or suspect that a customer (or a person on whose behalf a customer may be acting) is engaged in money laundering or terrorism financing, or if the transaction or the customer's conduct otherwise appears unusual or suspicious. These procedures must include arrangements for disciplining any member of staff who fails, without reasonable excuse, to make such a report.

The following are the procedures to be followed when reporting suspicious activity:

- Staff with any suspicion must report this immediately on the internal STR Form.
- The reason for the suspicion which is of utmost importance should be explained fully by the staff.
- The internal STR Form should be filled and sent to the MLRO who in turn will investigate and if found suspicious he/she will do an external reporting.

Under no circumstances whatsoever should the employee or the Placement Officer alert (i.e. "tip off") the customer that a report of suspicious activity has been initiated as this may constitute a criminal offence if the disclosure to the customer were to prejudice a subsequent investigation by the CBB.

All reports of suspicious activity must reach the MLRO, and only the MLRO has the authority to determine whether making a disclosure to the reporting authorities is appropriate. However, the Placement Officer is permitted to

add comments to the employee's suspicion report indicating any evidence as to why he/she believes the suspicion not to be justified.

11.3 EXTERNAL REPORTING BY THE MLRO

The MLRO will, upon receipt of a report concerning a suspicious customer or activity, determine whether the information contained in such report supports the suspicion. In this regard the MLRO should review the KYC records and historical transaction patterns and may also wish to discuss the report with members of staff and management.

- The MLRO will document his enquiries.
- If he has reason to suspect that a person has been engaged in money laundering this should be reported promptly to the reporting authorities.
- The MLRO will report to the Anti-Money Laundering Unit of the Ministry of Interior and the CBB's Compliance Directorate electronically using the Suspicious Transaction Reporting Online System (Online STR system).
- If the MLRO decides that the information does not substantiate a suspicion, he will record the reasons for deciding not to report to the respective reporting authorities in the MLRO Suspicion Evaluation Record.

The reports made by the MLRO or his duly authorized delegate must be sent electronically using the Suspicious Transaction Reporting Online System (Online STR system). to the relevant authorities of Bahrain at the following addresses:

Financial Intelligence Directorate (FID)
General Directorate of Anti Corruption and Economic and Electronic Security
Ministry of Interior
P.O. Box 26698
Manama, Kingdom of Bahrain
Telephone: + 973 17 749397
Fax: + 973 17 715502
E-mail: bahrainfid@moipolice.bh

Director of Compliance Directorate
Central Bank of Bahrain
P.O. Box 27
Manama, Kingdom of Bahrain
Telephone: 17547107
Fax: 17535673
E-mail: compliance@cbb.gov,bh

11.4 CONFIDENTIALITY OF SUSPICIOUS TRANSACTION REPORTS

Once a report has been made to the MLRO, all officers and employees of the Bank are prohibited from:

- Communicating directly or indirectly, in any manner or by any means to any person, the fact that the suspicious transaction report was made ('tipping off'); and

- Allowing publication or airing by the media, electronic mail or other similar devices in any manner or form the fact that a suspicious transaction was made.

- In cases where Islamic bank licensees form a suspicion that transactions relate to money laundering or terrorist financing, they must take into account the risk of tipping-off when performing the CDD process. If the Islamic bank licensee reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and must file an STR.

12. COMBATING THE FINANCING OF TERRORISM

The Bank must give special attention to any dealings they may have with entities or persons domiciled in countries or territories which are:

- Identified by the FATF as being "non cooperative"; or
- Notified to the Bank from time to time by the CBB.

Whenever transactions with such parties have no apparent economic or visible lawful purpose, their background and purpose must be re-examined and the findings documented.

If suspicions remain about the transaction, these must be reported to the reporting authorities.

The Bank must implement and comply with United Nations Security Council resolutions relating to the prevention and suppression of terrorism and terrorist financing. The Bank must freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity either (i) designated by, or under the authority of, the United Nations Security Council under Chapter VII of the Charter of the United Nations, including in accordance with resolution 1267(1999) and its successor resolutions as well as Resolution 2178(2014) or (ii) designated as pursuant to Resolution 1373(2001).

The Bank must comply in full with the provisions of the UN Security Council Resolution No. 1373 of 2001 ('UNSCR 1373'). DESIGNATED PERSONS AND ENTITIES

The CBB, from time to time, issues a list of designated persons and entities believed to be linked to terrorism. The Bank is required to verify that they have no dealings with these designated persons and entities, and report back their findings to the CBB. With respect to this requirement the Bank uses World-Check to ensure that both new and existing customers do not appear on the list of prohibited individuals and entities.

Names designated by the CBB include persons and entities designated by the United Nations, under UN Security Council Resolution 1267 ("UNSCR 1267").

The Bank must report to the relevant authorities, details of any accounts or other dealings with designated persons and entities, and comply with any subsequent directions issued by the CBB.

13. RECORD KEEPING

13.1 DOCUMENT RETENTION

The Bank will keep adequate records and identification documents for the following specific periods:

- In relation to evidence of identity and business relationship records, five years from the end of the Bank's relationship with the customer; and
- For transactions with customers transaction documents will be maintained for five years from the date when the transaction was completed.

All documents pertaining to customers must be retained for five years after the termination of relationship with such customer.

In addition, the following documents will be maintained for at least five years:

- Dates when AML training was provided, the nature of the training and the names of the staff who received the training;
- Reports made to, or by, the MLRO and records of consideration of those reports and any action taken as a consequence; and
- Compliance reports by the auditors.

All records must be available for prompt and swift access by the relevant authorities, when required.

14. EDUCATION AND TRAINING

The Bank will provide appropriate training to all employees. Such training will focus on:

- The identification and prevention of money laundering;
- Follow-up procedures for unusual or suspicious activities;
- Material changes in the applicable customer due diligence laws and regulations;
- Their responsibilities under the AML/CFT laws and regulations;
- The identity and responsibility of the MLRO;
- The current AML/CFT policies and procedures;
- Money laundering and terrorist financing typologies and trends;
- The type of customer activity or transaction that may justify an internal suspicious transaction report;
- The potential effect on the Bank, its employees and customers, of any breach of the AML Law or the AML/CFT Regulations;
- The procedures for making an internal suspicious transaction report; and
- Customer due diligence measures with respect to establishing new business relationships with customers.

The MLRO will be responsible for coordinating the necessary training and will maintain records of training courses and those employees who attend training.

The Bank is required to document and provide information to the CBB, when requested, that all relevant members of staff have received training on the matters listed above and that this training remains available to all relevant staff for so long as they work for the Bank.

The Bank is to provide up-to-date AML training for staff that is appropriate to the Bank's activities and its differing types of customers. Preferably, the AML training should be given to all staff on an annual basis. All staff must be given AML training within three months of joining the Bank.

15. ANNUAL COMPLIANCE REPORT

The Bank must take appropriate steps to identify and assess the money laundering and terrorist financing risks (for customers, countries or geographic areas; and products, services, transactions or delivery channels). And must document these assessments in order to be able to demonstrate the basis, keep these assessments up to date, and have appropriate mechanisms to provide risk assessment information to the CBB. The nature and extent of any assessment of money laundering and terrorist financing risks must be appropriate to the nature and size of the business.

The Bank will instruct suitable auditors to conduct a comprehensive annual review of the effectiveness of its AML controls and procedures at least once every year.

The scope of the review should include:

- A report indicating the number of internal STRs made in accordance with the CBB's regulations, including an analytical breakdown of all the results of those internal reports and their outcomes and whether controls, procedures or training need to be enhanced, made by the MLRO;

- A report which indicates the number of external STRs made in accordance with the CBB's regulations. The MLRO should ensure that where an internal report has been made without an external report, a justification is provided, made by the MLRO;

- A sample test of compliance with customer due diligence measures must be undertaken either by the Company's internal audit function or its external auditors; and

- A statement as to the quality of the Bank's AML procedures, systems and controls made by the external auditors.

The above information shall be submitted to senior management for review and for action to remedy deficiencies identified by the reports.

The CBB requires that the Bank instructs its external auditors to conduct the above annual review and report. The report must be submitted to the CBB by the 30th April of the following year.

At least two persons working on the report (one of whom should be the team leader) should have:
(a) A minimum of 5 years professional experience dealing with AML/CFT issues; and
(b) Formal AML/CFT training.

16. ACKNOWLEDGEMENT

I acknowledge that I have read and understood the provisions of the Bank's Anti-Money Laundering Policies and Procedures Manual.

Name of Employee: _____

Designation: _____

Signature: _____ Date: _____