Nona Marketing LTD

AML MANUAL

INDEX

Contents

PART I . . . 3

1. INTRODUCTION . . . 3

1.1 Duty to cooperate for prevention of Money Laundering and other criminal activities . . . 3

A. The role of the Board . . . 3

B. The role of the Senior Management . . . 4

1.2 Customer Due Diligence . . . 5

A. KYC Documentation for natural persons . . . 8

B. KYC Documentation for corporate customers . . . 10

C. KYC Documentation for partnerships and unincorporated business . . . 11

D. KYC Documentation for other legal structures and fiduciary arrangements . . . 11

E. KYC Documentation for trust clients . . . 12

F. KYC Documentation for foundations . . . 12

G. KYC Documentation for Executorship Accounts . . . 12

1.3 Certification of Customer Information . . . 12

1.4 Customers' Profile Policy . . . 12

1.5 Risk based approach . . . 13

A. Simplified customer due diligence . . . 14

B. Enhanced customer due diligence . . . 14

1.6 Other obligations of the Company . . . 15

1.7 Reporting of suspicious transactions by the Company . . . 16

1.8 Company to appoint a compliance officer and establish procedures, etc . . . 17

PART I

INTRODUCTION

Nona Marketing LTD (hereinafter the "Company") is committed to the highest standards of the Anti-Money Laundering (AML) compliance and Anti-Terrorist Financing and requires the management, and employees to fully observe and follow the named standards. The Company therefore takes all necessary measures to detect and counter money laundering and terrorism financing. The internal rules are observed in accordance with the relevant international requirements

1. AML POLICY

1.1 **Duty to cooperate for prevention of Money Laundering and other criminal activities**

i. The Company shall determine the identity of the beneficial ownership of all their clients' accounts and shall not open or maintain such accounts, unless they are satisfied of this requirement.

ii. The Company shall take all reasonable measures to ensure that accounts are not used for the purpose of holding assets obtained as the result of, or for facilitating the commission of any criminal activity.

iii. The Company shall develop and implement policies and procedures to identify and avoid money laundering transactions and to ensure compliance with the relevant international requirements.

iv. The Company shall, on a regular basis, evaluate the effectiveness of their policies and control procedures in complying with the international requirements and any relevant guidelines, and such evaluation shall be an integral component of any internal audit.

v. The Company shall be vigilant in ensuring the prevention of their involvement or misuse in money laundering activities, and shall not knowingly accept assets or enter into business relationships where there is reasonable cause to believe that such assets may have been acquired illegally or that they represent the proceeds of criminal activity.

The Company shall establish procedures to obtain appropriate evidence of client identity, and shall maintain adequate records of client identity and transactions involved in such a manner as to assist, if necessary, in the investigation of criminal offences.

A. **The role of the Board**

i. The Board has the ultimately responsibility for the effectiveness of the Company's AML framework. The Board's oversight role is intended to ensure, inter alia, that there is compliance with all the relevant international laws and regulations. Such compliance should assist in the detection of suspicious transactions and permit the creation of an audit trail if an investigation is deemed necessary.

ii. The Board should therefore demonstrate its commitment to an effective AML programme by:

a. Understanding the AML and Anti-Terrorist Financing standards placed upon it, their staff

and the entity it represents;

b. Approving AML policies and procedures that are appropriate for the risks faced by the Company. Evidence of consideration and approval of these policies should be reflected in the board minutes and noted in the policy;

c. Appointing an individual within the organization to ensure that the Company's AML procedures are being managed effectively; and

B. **The role of the Senior Management**

i. Senior management is responsible for the development of sound risk management programmes and for keeping the Board adequately informed about these programmes and their effectiveness. These programmes, which should be designed to permit a sound knowledge of a customer's business and pattern of financial transactions and commitments, should be formally documented and, at a minimum, irrespective of whether the Company receives funds from third parties or not, should provide for:

a. The development of internal policies, procedures and controls for, inter alia:

ii. The opening of customer accounts and verification of customer identity;

iii. Establishing business relations with third parties (including custodians, fund managers, correspondent banks, business introducers);

iv. Determining business relationships that the financial institution will not accept by requiring graduated customer acceptance policies and procedures with more extensive due diligence for higher risk customers;

v. Determining an exit strategy to terminate undesired relationships with existing customers;

vi. The timely detection of unusual activities and reporting of suspicious transactions;

vii. Internal reporting; and

viii. Records retention.

i. The recruitment of a level of staff, appropriate to the nature and size of the business, to carry out identification, research of unusual transactions and reporting of suspicious activities;

j. Designation of a compliance officer at an appropriate level of authority, seniority and independence to coordinate and monitor the compliance program;

k. An ongoing training programme designed to ensure employees adhere to the internal procedures and become familiar with the dangers they and the business entity face and on how their job responsibilities can encounter specified money laundering and terrorist financing risks;

l. Establishment of management information/reporting systems to scrutinize customer account activity and facilitate aggregate and group-wide monitoring of significant balances

regardless of whether the accounts are held on balance sheet, as assets under management or on a fiduciary basis;

m. An effective independent risk-based oversight function to test and evaluate the compliance program; and

n. Screening procedures for hiring, and ongoing systems to promote high ethical and professional standards to prevent the financial institution from being used for criminal activity. This should include but is not limited to enquiries about the personal history of the potential employee and verifying appropriate references on the individual.

ii. Policies should be periodically reviewed for consistency with the business model, and product and service offering. Special attention should be paid to new and developing technologies.

1.2 Customer Due Diligence

i. The Company shall establish the identity and verify the identity of any customer of the Company by requiring the customer to produce an identification record or such other reliable, independent source document.

ii. The obligation to identify customers exists if the customers proceed with the following:

a. Opens an account with a reporting entity

b. Engages the services of a reporting entity;

c. Enters into a business relationship with a reporting entity.

iii. The Company must carry out a prescribed identification process on:

a. a person conducting a transaction

b. a person whose behalf a transaction is being conducted

c. a beneficial owner.

iv. The requirements of subsection (i) shall apply when:

a. The reporting entity carries out an electronic currency transfer for the Customer,

b. Suspects that the Customer is involved in proceeds of crime, a financing of terrorism or a serious offence,

c. Suspects that the transaction involves proceeds of crime, or may be used for financing terrorism or for committing a serious offence or

d. There are doubts on the veracity or adequacy of the customer identification or information that had previously obtained.

v. The requirements of subsection (i) shall apply when:

a. the Company establishes a business relationship;

b. in the absence of such a relationship, the Company conducts: any transaction in an amount equal to or above the sum of $15.000 or such other amount as may from time to time be prescribed by the Minister, whether conducted as a single transaction or several transactions that appear to be linked and where the amount of the transaction is unknown at the time of the transaction, the identification and verification shall be undertaken as soon as the amount becomes known or the said threshold is reached;

c. there is a suspicion of money laundering or terrorist financing; or

d. the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

vi. Generally, a financial institution should not accept funds from prospective customers unless the necessary verification has been completed. In exceptional circumstances, verification of customer identity and beneficial owner may be undertaken following the establishment of the business relationship provided that:

a. It is done as soon as reasonably practicable

b. It would be essential not to interrupt the normal conduct of business (e.g. non face to-face business and securities transactions)

c. The money laundering risks are effectively managed. Should a financial institution determine this to be an unacceptable risk, they should retain control of any funds received until verification requirements have been met.

Where a customer is permitted to utilize the business relationship prior to verification, financial institutions should adopt risk management procedures under which this may occur. These procedures should include a set of measures on the limitation of the number, types and/or amount of transactions that can be performed and the monitoring of large or complex transactions outside of the expected norm for the type of relationship.

vii. Without limiting the generality of subsection (i), the Company shall:

a. When establishing a business relationship, obtain information on the purpose and nature of the business relationship and the source of funds;

b. if the transaction is conducted by a natural person, adequately identify and verify his identity including information relating to:

- the person's name and address;
- the national identity card, social security document, passport or other applicable official identifying document;
- the source of funds;

c. if the transaction in conducted by a legal person or legal arrangement, obtain

information on that legal person or legal arrangement, adequately identify the company, the beneficial owner and ultimate natural persons providing the funds of such legal person or legal arrangement and take reasonable measures to identify and verify the legal status, ownership and control structure, including information relating to:

- proof of incorporation or similar evidence of establishment or existence; and;
- the customer's name, name of trustee and ultimate settler (for trusts) and of persons providing funds and council members (for foundations), legal form, head office address and identities of directors (for legal persons) and source of funds;

d. have appropriate risk management systems to determine if a potential customer, customer or beneficial owner is, is likely to be, is found to be or becomes a politically exposed person, and if so, shall:

- adequately identify and verify his identity as set out in this section;
- obtain the approval of senior management before establishing or continuing a business relationship with the politically exposed person;
- take reasonable measures to establish the source of funds and source of property; and
- conduct regular enhanced ongoing monitoring of the business relationship.

"politically exposed person" means any individual who is or has been entrusted with prominent public functions in the Republic of Marshall Islands or in another country or territory, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials including family members or close associates of the politically exposed person.

e. perform due diligence measures on a risk sensitive basis; and

f. upon the establishment of a business relationship, and when completing the verification of the identity of the customer and beneficial owner, ensure that money laundering risks are effectively managed.

viii. The Company shall, in relation to its higher risk category of customers or business relationship, conduct annual reviews of its record to ensure that the documents, data or information obtained pursuant to subsection (vii) is kept up-to-date and relevant.

ix. If it appears to the Company that an applicant requesting it to enter into any business relationship or transaction, whether or not in the course of a continuing business relationship, is acting on behalf of another person, the Company shall establish the true identity of any person on whose behalf or for whose ultimate benefit the applicant may be acting in the proposed transaction, whether as a trustee, nominee, agent or otherwise.

x. Nothing in this section shall require the production of any evidence of identity where:

a. the customer is itself a financial institution to which the legislative applies and which has been licensed or registered, and is supervised for anti-money laundering and countering the financing of terrorism measures by a regulatory authority and the Company has satisfied itself as to the adequacy of the measures to prevent money laundering and the financing of terrorism; or

b. there is a transaction or a series of transactions taking place in the course of a business relationship, in respect of which the applicant has already produced satisfactory evidence of identity.

xi. The Company does not rely on an intermediary or third party to undertake its obligations under subsections (i), (i) or (iii) or to introduce business to it.

xii. The Company does not accept anonymous accounts or accounts in fictitious names.

xiii. As part of the due diligence process, a financial institution should:

a. Use reasonable measures to verify and adequately document the identity of the customer or account holder at the outset of a business relationship. This process should include, where appropriate:

ii. Taking reasonable measures to understand the ownership and control structure of the customer;

iii. Obtaining information on the purpose and intended nature of the business relationship, the source of funds, and source of wealth, where applicable; and

iv. Discontinuing the transaction, if customer documentation information is not forthcoming.

e. Employ enhanced due diligence procedures for high risk customers or transactions or business relationships such as private banking operations, non-resident customers, trust arrangements, companies having nominee shareholders or customers who the financial institution has reasons to believe are being refused banking facilities by another financial institution;

xiv. When an existing customer closes one account and opens another, or enters into a new agreement to purchase products or services, there is no need to re-verify identity or address. However, the opportunity should be taken to confirm the relevant customer information. This is particularly important when a previously dormant account has been reactivated or if there has been no recent contact or correspondence with the customer within the last 12 months.

A. **KYC Documentation for natural persons**

i. The Company must obtain and document the following basic information when seeking to verify identity:

a. True name/names used and correct permanent residential address including postcode

(if applicable);

b. Valid photo-bearing identification, with unique identifier, (e.g. passport, social security card or driver's license along with a passport or social security card);

c. Date and place of birth and nationality (indication should be made if dual citizenship is maintained);

d. Contact details e.g. telephone number, fax number and e-mail address;

e. Signature;

f. Purpose of the account and the nature of the business relationship.

ii. The following information may also be required when the Company seeks to verify identity:

a. Occupation and name of employer (if self-employed, the nature of the self-employment);

b. Estimated level of account activity including:

1. Size in the case of investment and custody accounts;

2. Balance ranges, in the case of current and deposit accounts;

3. An indication of the expected transaction volume of the account;

c. Source of funds; and

d. Any other information deemed appropriate and relevant.

iii. Identification documents, either original or certified copies, should be pre-signed and bear discernible photograph of the applicant, for example:

a. Current valid passport;

b. Armed forces ID card;

c. Driver's license bearing the photograph and signature of the applicant (to be used along with a passport or social security card);

d. Voter's card;

e. Social security card; or

f. Such other documentary evidence as is reasonably capable of establishing the identity of the individual customer.

iv. One or more of the following steps used in order to confirm customer's addresses:

a. Checking the Register of Electors;

b. Provision of a recent utility bill, tax assessment or bank or credit union statement containing details of the address (to guard against forged copies it is strongly recommended

that original documents are examined);

c. Checking the telephone directory; and

d. Record of home visit.

v. Where prospective customers provide documents with which a financial institution is unfamiliar, either because of origin, format or language, the financial institution must take reasonable steps to verify that the document is indeed authentic, which may include contacting the relevant authorities or obtaining a notarized translation.

vi. In circumstances where the Company's customer is considered a high risk client, the Company should also take reasonable measures to establish the customer's source of wealth and document findings.

vii. Where a customer is unable to produce original documentation needed for identification or verification, copies should be accepted if certified by persons listed in section 11.5 of this manual.

B. **KYC Documentation for corporate customers**

i. To satisfy itself as to the identity of the corporate customer, the Company obtain:

a. Name of corporate entity;

b. Principal place of business and registered office;

c. Mailing address;

d. Contact telephone and fax numbers;

e. Board resolution authorizing the opening of the account and conferring authority on signatories to the account;

f. An extract from the Commercial Register, or equivalent document, evidencing the registration of corporate acts and amendments;

g. Satisfactory evidence of the identity of all account signatories, details of their relationship with the company and if they are not employees, an explanation of the relationship. All signatories must be verified in accordance with the identification and verification of identity requirements of natural persons;

h. Identity information on the natural persons with a controlling interest in the corporate entity. This information should extend, as far as practicable, to identifying those with a minimum of 10% shareholding, those who ultimately own and have principal control over the company's assets, including anyone who is giving instructions to the financial institution to act on behalf of the company. However, if the company is publicly listed on a recognized stock exchange and not subject to effective control by a small group of individuals, identification and verification of the identity of shareholders is not required;

i. Confirmation before a business relationship is established, by way of company search and/or other commercial enquiries that the applicant company has not been, or is not in the

process of being dissolved, struck off the companies register, wound-up or terminated. Such confirmation may be verified by obtaining a current Certificate of Good Standing or equivalent document or alternatively, obtaining a set of consolidated financial statements that have been audited by a reliable firm of auditors and that show the group structure and ultimate controlling party;

ii. Therefore, the Company obtains the following information and documents when seeking to verify the identity of corporate customers:

a. Certified Copy of the Memorandum and Articles of Association of the entity;

b. Description and nature of business, including date of commencement, products or services provided, location of principal business and name and location of the registered office and registered agent of the corporate entity, where appropriate;

c. Purpose of the account, the estimated account activity (including volume, balance ranges in the case of current and deposit accounts; size in the case of investment and custody accounts), source of funds and source of wealth in circumstances where the financial institution's customer is considered high risk;

d. By-laws and any other relevant corporate documents filed with the Companies' Registry;

e. Recent financial information or audited statements;

f. Copies of Powers of Attorney, or any other authority, affecting the operation of the account given by the directors in relation to the company and supported by a copy of the respective Board Resolution;

g. Copies of the list/register of directors and officers of the corporate entity including their names and addresses;

h. Written confirmation that all credits to the account are and will be beneficially owned by the facility holder except in circumstances where the account is being operated by an intermediary for the purpose of holding funds in his professional capacity;

i. Satisfactory evidence of identity must be established for at least two directors, one of whom should, if applicable, be an executive director where different from account signatories; and

j. Such other official documentary and other information as is reasonably capable of establishing the structural information of the corporate entity.

C. **KYC Documentation for partnerships and unincorporated business**

The Company does not accept this type of customer.

D. **KYC Documentation for other legal structures and fiduciary arrangements**

The Company does not accept this type of customer.

E. **KYC Documentation for trust clients**

a. In the case of a nominee relationship, obtain identification evidence for the beneficial owner(s).

F. **KYC Documentation for foundations**

The Company does not accept this type of customer.

G. **KYC Documentation for Executorship Accounts**

The Company does not accept this type of customer.

1.3 **Certification of Customer Information**

i. The Company should exercise due caution when considering certified documents, especially where such documents originate from a country perceived to represent a high risk, or from unregulated entities in any jurisdiction. Where certified copy documents are accepted, it is the Company's responsibility to satisfy itself that the certifier is appropriate. In all cases, a financial institution should also ensure that the customer's signature on the identification document matches the signature on the application form, mandate, or other document.

ii. For natural persons, face-to-face customers must, where possible, show the Company's staff original documents bearing a photograph and copies should be taken immediately, retained and certified by a senior staff member.

iii. Where it is impractical or impossible to obtain sight of original documents, a copy is acceptable where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the facility holder.

iv. A certifier must be a qualified practicing notary public or attorney-at-law.

v. The certifier should sign the copy document (printing his name clearly underneath) and clearly indicate his position or capacity on it together with a contact address, telephone and facsimile number and where applicable, a license/registration number.

1.4 **Customers' Profile Policy**

i. A customer profile policy is determined and implemented under particular criteria related with clients' risk profile. In particular, the factors that specify the risk category at which a client is attributed are mainly dealing with client:

ii. The nature of the customer's business (whether cash intensive e.g. casinos and restaurants);

a. The nature and frequency of the activity;

b. The complexity, volume and pattern of transactions;

c. Type, status and value of account;

d. Type of customer, based on specific risk factors (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place);

e. Type of product/service (e.g. whether private banking, one-off transaction, mortgage);

f. Delivery channels (e.g. whether internet banking, wire transfers to third parties, remote cash withdrawals);

g. Geographical origin of the customer;

h. Geographical area (e.g. whether business is conducted in or through jurisdictions with high levels of drug trafficking, corruption or lacking proper standards in the prevention of money laundering/financing of terrorism, whether the customer is subject to regulatory or public disclosure requirements);

i. Whether the origin of wealth and/or source of funds can be easily verified and whether the audit trail has been deliberately broken and/or unnecessarily layered;

j. Unwillingness of the customer to cooperate with the financial institution's customer due diligence process for no apparent reason;

k. Any other information that raises suspicion of the customer's connection to money laundering or terrorist financing.

1.5 **Risk based approach**

i. The Company's risk-based approach requires an assessment of the risk posed by the nature of the business and the implementation of appropriate mitigation measures, while maintaining an overall effective programme. This should be evidenced by categorization of the customer base, products and services by risk rating and identification of assigned actions by risk types.

ii. Prior to establishing a business relationship, the Company should assess the potential risk inherent in each new client relationship. This assessment should take into account the products or facilities to be used by the customer and whether and to what extent a customer may expose the Company to risk. The financial institution should then decide whether or not to establish or continue with a relationship.

iii. The Company categorises customers in terms of risk in 3 groups, namely:

a. Low Risk

b. Medium Risk

c. High Risk

iv. The Company's risk based approach take into account customer acceptance and on-going monitoring policies and procedures that assist the Company in identifying the types of customers that are likely to pose higher than average money laundering and terrorist financing risk.

v. The Company is required to risk rate all client relationships including those in existence prior to the implementation of these Guidelines. All risk ratings should be documented and should be in place for all customers.

vi. The Company adopted reasonable criteria for assessing the risks (e.g. whether ownership of a corporate customer is highly complex for no apparent reason, whether the customer is a PEP, whether the customer's employment income supports account activity, whether customer is known to other members of the financial group, whether delegated authority such as power of attorney is in place).

vii. The Company conducts periodic reviews (however, not more than two years apart) to determine whether any adjustment should be made to its risk rating. The review of the risk rating for high risk customers may be undertaken more frequently than for other customers and a determination should be made by senior management as to whether the relationship should be continued. All decisions regarding high risk relationships and the basis for these decisions should be documented.

A. **Simplified customer due diligence**

i. Reduced due diligence is acceptable for example, where information on the identity of the customer or beneficial owner is publicly available or where checks and controls exist elsewhere in national systems.

B. **Enhanced customer due diligence**

i. A more extensive customer due diligence process should be adopted for higher risk customers. In particular, the Company applies enhanced due diligence to customers where the risk of being used for money laundering or terrorist financing is high. It follows, then, that simplified customer due diligence measures are not acceptable whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios apply.

ii. The Company may determine that a customer is high risk because of the customer's business activity, ownership structure, nationality, residence status, anticipated or actual volume and types of transactions. A financial institution may be wary of doing business with persons from countries where, for example, it is believed that there is a high level of drug trafficking or corruption and greater care may be needed in establishing and maintaining the relationship or accepting documentation from such countries.

iii. Applying a risk-based approach, enhanced due diligence for high risk accounts may include, where deemed relevant, and with more frequency than applied for low risk customers:

a. An evaluation of the principals;

b. A review of current financial statements;

c. Verification of the source of funds;

d. Verification of source of wealth;

e. The conduct of reference checks;

f. Checks of electronic databases and

g. Periodic reporting to the Board about high risk accounts.

iv. The Company should give particular attention to the following business relations and transactions:

a. Where a customer has not been physically present for identification purposes;

b. Correspondent relationships;

c. Business relationships or occasional transactions with a PEP;

d. Business relations and transactions with persons from or in countries and jurisdictions known to have inadequate AML measures;

e. Corporate customers able to issue bearer shares or bearer instruments.

v. In particular, the Company defines the following types of customers as high risk clients and therefore enhanced due diligence are applied:

a. Non-Face to Face Customers

b. Politically Exposed Persons

c. High-Risk Countries

1.6 Other obligations of the Company

i. The Company shall establish and maintain the following:

a. records of all transactions in accordance with the requirements of subsection (iii) below

b. where evidence of a person's identity is obtained, a record that indicates the nature of the evidence obtained, and which comprises either a copy of the evidence or such information as would enable a copy of it to be obtained;

c. account files and business correspondence in relation to accounts;

ii. Customer accounts of the Company shall be kept in the true name of the account holder.

iii. Records required under subsection (i) shall contain particulars sufficient to identify:

a. the name, address and occupation or, where appropriate, business or principal activity of each person

- conducting the transaction; or
- if known, on whose behalf the transaction is being conducted, as well as the method used by the Company to verify the identity of each such person;

b. the nature and date of the transaction;

c. the type and amount of currency involved;

d. the type and identifying number of any account with the Company involved in the

transaction;

e. if the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee, if any, the amount and date of the instrument, the number, if any, of the instrument and details of any endorsements appearing on the instrument;

iv. Records required under subsection (i) shall be kept by the Company for a period of at least 6 years from the date the relevant business or transaction was completed, or termination of business relationship or any longer period in specific cases and upon proper authority and the requirement to keep the record shall apply whether the account or business relationship is ongoing or has been terminated. In addition,

a. The Company shall keep such records of a transaction that are sufficient to permit reconstruction of individual transactions;

b. Any record kept under this section, shall be maintained in a manner for use as evidence for prosecution of an offence.

v. The Company must keep:

a. A record of any suspicious transaction, suspicious activity or other report;

b. A record of any enquiry relating to money laundering or the financing of terrorism made to the Director;

c. A record of a findings.

vi. The Company shall ensure that customer information and transaction records are available on a timely basis to domestic authorities upon proper authority.

vii. The Company is prohibited from conducting any banking business such as receiving money from the public through the acceptance of deposits on current account, deposit account or other similar accounts which may be withdrawn on demand by cheque, draft, order or notice by customers and using that money to make advances, loans, extensions of credit, guarantees and investments.

1.7 **Reporting of suspicious transactions by the Company**

i. The Company shall pay special attention to:

a. all complex, unusual or large business transactions, or unusual patterns of transactions, whether completed or not, and to insignificant but periodic transactions, that have no apparent economic or lawful purpose;

b. business relations and transactions with persons including legal persons and arrangements, from or in jurisdictions that do not have adequate systems in place to prevent or deter money laundering or terrorist financing;

c. electronic funds transfer that do not contain complete originator information and shall adopt effective risk-based procedures to identify and handle any such transfer.

ii. In relation to subsection (i), the Company shall:

a. set forth in writing the specific information regarding the transaction(s) or business relations specified in subsection (i) (a) to (c) of this section, its background and purpose to the extent known, and the identity of the persons involved

iii. The Company shall conduct ongoing due diligence on its business relationships and scrutinize transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with information that the Company has of its customer and the profile of the customer's business and where necessary the source of funds.

iv. Whenever the Company suspects or has reasonable grounds to suspect that any transaction, proposed transaction or attempted transaction is related to the commission of a money laundering offence or terrorist financing offence or is related or linked to, or is to be used in connection with a terrorist act or for the financing of terrorism, or that the funds or property are the proceeds of crime, it shall as soon as possible but not later than 1 days after forming that suspicion and wherever possible before the transaction is carried out:

a. take reasonable measures to ascertain the purpose of the transaction, the origin and ultimate destination of the funds involved and the identity and address, of any ultimate beneficiary;

b. prepare a report of the transaction in accordance with subsection (v);

v. Overall a company shall report any suspicious transaction or activity, and/or any large cash transactions that may be out of the scene.

vi. A report required shall:

a. set forth all particulars known regarding the transaction;

b. contain a statement of the grounds on which the Company holds the suspicion; and

c. be signed or otherwise authenticated by the Company.

vii. The form of the report can be either oral or written. If the report is oral (including telephone communication) then a written report shall follow within the next 24 hours.

viii. A report must be submitted either by fax, email and/or hand delivery.

1.8 **Company to appoint a compliance officer and establish procedures, etc**

i. The Company shall:

a. appoint a compliance officer who shall be responsible for ensuring the Company's compliance with the international requirements;

b. establish and maintain internal policies, procedures, controls and systems to:

- implement the customer identification requirements;

- implement record keeping and retention requirements;
- implement the monitoring requirements;
- implement the reporting requirements;
- make its officers and employees aware of the laws relating to combating money laundering and financing of terrorism. In particular, the law on customer due diligence and suspicious transaction reporting;
- make its officers and employees aware of the procedures and policies adopted by it to deter money laundering and the financing of terrorism;
- screen persons before hiring them as employees;
- disseminate warning notices and other information received from the competent authority relating to a weakness in the anti-money laundering and combating of financing of terrorism systems of other countries; and

c. conduct ongoing training of its officers, employees and agents to ensure that employees are kept informed of new developments, including information on current money laundering and terrorist financing techniques, methods and trends.

ii. The Company shall:

a. enable any person identified in accordance with subsection (i) (a) as well as other appropriate staff to have timely and unimpeded access to information that may be relevant to determining whether sufficient basis exists to report the matter; and

b. require the identified person to report the matter in the event that he determines that sufficient basis exists.

iii. The person identified in subsection (i) (a) shall:

a. be of an officer of a rank at management level or above with relevant qualifications and experience to enable him to respond sufficiently well to inquiries relating to the Company and the conduct of its business and possess core competencies and knowledge in administering anti-money laundering measures;

b. be responsible for establishing and maintaining such manual of compliance procedures in relation to its business;

c. be responsible for ensuring compliance by staff of the Company with:

- any law relating to money laundering or terrorist financing; and
- any manual of compliance procedures established;