BMFN LIMITED

MANUAL FOR THE

PREVENTION AND SUPPRESSION OF

MONEY LAUNDERING AND

TERRORIST FINANCING

Introduction

BMFN Limited (hereinafter "the Company") is fully committed to the fight against financial crime. To this end, the company has employed a robust and efficient approach in the area of Anti-money laundering, regulations, suspicious activity reports, Know your customer (KYC), Customer due diligence and Enhanced Due Diligence, Risk assessments, transaction monitoring, and investigations.

The purpose of this procedures manual is to establish the below processes to be followed:

1. Create a corporate culture of "Know your Customer" (KYC) as well as to take the appropriate measures for the prevention of Money Laundering and Terrorist Financing
2. To establish the basic principles of the Company for the prevention of Money Laundering and Terrorist Financing
3. Establish a common procedure so that the prevention of Money laundering and Terrorist Financing is effective
4. Recognize and report suspicious transactions and activities to the Authority for combating money laundering (hereinafter "the Authority")
5. Establish procedures for customer identification and due diligence
6. Train and update the employees of the Company on any developments regarding the prevention of Money laundering and Terrorist Financing

1. INTERNAL CONTROL PROCEDURES AND RISK MANAGEMENT

1.1. Obligation to establish procedure

The company has established adequate and appropriate systems and procedures for the following:

1.1.1. Internal control, risk assessment and risk management in order to forestall and prevent money laundering and terrorist financing, and

1.1.2. the detailed examination of any transaction which by nature may be considered to be particularly vulnerable to be associated with money laundering or terrorist financing, and in particular, complex and unusually large transactions and all unusual patterns of transactions which have no apparent economic or clear lawful purpose.

2. THE ROLE OF THE MONEY LAUNDERING COMPLIANCE OFFICER

2.1. Appointment of a Money Laundering Compliance Officer ("MLCO ")

The Director(s) appoints a senior staff member who has the skills, knowledge and expertise in financial or other activities, as the case may be, known as the MLCO to whom a report is to be made

about any information or other matter which comes to the attention the Company and which, in the opinion of the person handling that business, proves or creates suspicions that another person is engaged in money laundering or terrorist financing;

2.2. **Duties of the Money Laundering Compliance Officer**

(i) The MLCO has the responsibility, to record and assess on an annual basis all risks arising from existing and new customers, products and services as well as the measures or changes to the systems and procedures implemented by the company for the effective management of the aforesaid risks.

(ii) The MLCO prepares the Customer Acceptance Policy/form

(iii) The MLCO has the primary responsibility for the preparation of the company's risk management and procedures manual for the prevention of money laundering and terrorist financing. The manual is assessed on a periodic basis and reviewed when deficiencies are found or when the need arises to adapt the company's procedures for the effective management of the risks emanating from money laundering and terrorist financing.

(iv) The MLCO monitors and assesses whether the policy, procedures and controls that have been introduced for the prevention of money laundering and terrorist financing are correctly and effectively applied.

(v) The MLCO receives any information from the company's employees which is considered by the latter to be knowledge or suspicion of money laundering or terrorist financing activities or might be related with such activities in the form of an internal report. A specimen of this internal report (hereinafter to be referred to as "Internal Money Laundering Suspicion Report") is attached, as Appendix 1, to this manual. All such reports should be registered and kept on a separate file.

(vi) The MLCO evaluates and investigates the information received. The evaluation of the information reported to the MLCO should be made on a separate form which should be registered and retained on file. A specimen of this report (hereinafter to be referred to as "Money Laundering Compliance Officer's Internal Evaluation Report") is attached, as Appendix 2, to this manual.

(vii) If following the evaluation described in paragraph (vi) above, the MLCO decides to notify the Authority, then he/she should complete a written report and submit it the soonest possible. All such reports should be registered and kept on a separate file.

(viii) After the submission of the MLCO's report to the Authority, the transactions of the customer(s) involved are monitored by the MLCO.

(ix) If following the evaluation described in paragraph (vi) above, the MLCO decides not to notify the Authority, then he/she should fully explain the reasons for such a decision on the "Money Laundering Compliance Officer's Internal Evaluation Report" which should, as already stated, be registered and retained on file.

(x) The MLCO maintains a registry with statistical information (e.g. date of submission of the internal report, date of assessment, date of reporting to the Authority) in relation to the Internal Money Laundering Suspicious Reports and the MLCO's reports to the Authority.

(xi) The MLCO provides advice and guidance to the employees of the company on the correct implementation of procedures and controls to prevent money laundering and terrorist financing.

(xii) The MLCO determines which of the company's employees need further training and education for the purpose of money laundering and terrorist financing prevention and organizes appropriate training sessions/seminars. In this regard, the MLCO prepares and applies, an annual staff training program.

(xiii) The MLCO maintains a register with the data/information (i.e. name, place of business, area of activity, supervisory authority, date of commencement of business relationship, last review date, next review date, rating) of the third person with whom the company has established a business relationship.

3. THE APPLICATION OF APPROPRIATE MEASURES AND PROCEDURES ON A RISK SENSITIVE BASIS

3.1. Introduction

The Company applies customer identification and due diligence procedures on a risk based approach depending on the type of customer, business relationship, product or transaction. However, the company must be able to demonstrate that the extent of the measures is commensurate with the risks from the use of their services for the purposes of money laundering and terrorist financing.

Applying measures and procedures on a risk sensitive basis enables companies to focus their efforts on those areas where the risk of money laundering and terrorist financing appears to be higher.

3.2. Identifying and Assessing Risks

A risk-based approach starts with the identification, recording and assessment of the risk that has to be managed. The identification and assessment of risk entails answering the following questions:

- What risk is posed by the company's customers?
- What risk is posed by a customer's behavior (e.g. customer transactions where there is no apparent legal/financial/commercial rationale).
- What risk is posed by the products/services the customer is using? (e.g. making payments via electronic funds transfers, large cash deposits or withdrawals, investment products etc.).

Indicative parameters of a risk based system of controls and procedures are the following:

- The nature and profile of customers as well as of products and services offered.
- The volume and size of transactions.
- The country of origin and destination of customers' funds.

- Deviations from the anticipated level of transactions.
- The nature of business transactions.

3.3. **Design and implementation of controls to manage and mitigate the risks**

Once the Company has identified the risks it faces then it designs and implements the appropriate systems and controls for their management and mitigation in accordance with the procedures prescribed in this manual. As regards money laundering and terrorist financing, managing and mitigating the risks involves measures to verify the customer's identity, collecting additional KYC information about the customer to construct his business profile and monitoring his transactions and activity.

In order to ensure its policies, procedures and controls on anti-money laundering and terrorist financing are appropriate and effective, having regard to the assessed risk, the company determines the type and extent of measures it should adopt, to manage and mitigate the identified risks cost-effectively. These measures may, for example, include:

- Adapting the customer due diligence procedures in line with their assessed money laundering and terrorist financing risk;
- Obtaining additional customer or business relationship data and information where this is appropriate for the proper and complete understanding of a customer's activities and source of wealth to effectively manage any increased risk emanating from the particular business relationship.
- On-going monitoring of high risk customers' transactions and activities (where applicable)

The risk assessment and the implementation of the aforementioned measures must result in the classification of customers into three risk categories: low, normal and high risk. Criteria will be attached to each category to reflect the possible risk and each category should be accompanied by the corresponding due diligence procedures, periodic monitoring and controls. Enhanced customer due diligence measures should be applied on a risk sensitive basis, in all business relationships which by nature present a higher risk of money laundering or terrorist financing.

3.4. **Dynamic Risk Management**

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Systems and controls should be kept under regular review so that risks resulting from changes in the characteristics of existing customers, new customers, products and services and in the geographical dispersion are managed and countered effectively.

4. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES

4.1. **Introduction**

Collecting and maintaining sufficient information about a customer, making use of that information for the purposes of customer identification is the basis of all other procedures for the prevention of money laundering and terrorist financing and is the most effective weapon against the possibility that the services provided by company are used for the above mentioned illegal purposes. In addition to minimize the risk of a company's services being used for illicit activities, collecting and maintaining sufficient information on a customer's identity allows the early detection and recognition of suspicious transactions/activities and protects the company from possible fraud and the underlying risks to their reputation

4.2. **Customer identification and due diligence procedures**

Customer identification and due diligence procedures, include the following:

(i) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(ii) identifying the beneficial owner and taking risk-based and adequate measures to verify his identity based on documents, records or information issued or obtained from an independent, reliable source.

(iii) Conducting ongoing monitoring of the business relationship, including scrutiny of transactions carried out throughout the course of that relationship, to ensure that these transactions are consistent with the information and data in the possession of the person engaged in financial or other business activities in relation to the customer, the business and risk profile, and ensuring that the documents, data or information held are kept up-to-date (where applicable).

The purpose of determining customer identification and due diligence measures, the proof of identity is sufficient if it is reasonably possible to establish that the applicant/customer is the person he claims to be.

4.3. **Timing of identification**

The verification of the identity of the customer and the beneficial owner(s) is to be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is low risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact and before the withdrawal of funds.

4.4. **Exercise of due diligence and updating of identification data of existing customers**

The Company applies customer identification and due diligence measures when there are doubts about the veracity or adequacy of previously obtained customer identification documents, data or

information. Furthermore, the application of customer identification and due diligence procedures is applied not only to new customers but also at appropriate times, and where applicable , to existing customers, depending on the level of risk of being involved in money laundering or terrorist financing activities.

The company ensures that their customer identification records as well as the information that form their business/economic profile remain updated throughout the business relationship. In this respect, the company examines and checks on a regular basis the validity and adequacy of the customer identification data and information maintained, especially those concerning high-risk customers. The policy and the procedures for the prevention of money laundering determines the timeframe during which the regular review, examination and update of the customer identification data is conducted, depending on the risk categorization of each customer.

Despite the above and taking into account the level of risk, if at any time during the business relationship with an existing customer, a company becomes aware that reliable or adequate data and information are missing from the identity of the customer, then the company takes all necessary action, by applying the customer identification and due diligence procedures, to collect the missing data and information, the soonest possible, so as to update and complete the customer's information.

In addition to the update of the customer identification data and information on a regular basis or when it is observed that unreliable or inadequate data and information are being held, the company checks the adequacy of the data and information held with regard to the customer's identity and business/economic profile, whenever one of the following events or incidents occurs:

(1) An individual transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the business/economic profile of the customer.

(2) Customer's reclassification (e.g. low risk customers to normal or high risk).

(3) In case of identification of negative information about the client in the press or the internet or information submitted by a competent supervisory authority or a credit institution or following investigation which points to the need for an update of the data and information about the customer or to a possible risk reclassification.

If a customer fails or refuses to submit, within a reasonable timeframe, the required data and identification information for the updating of his/her identity and business/economic profile and, as a consequence, the company is unable to comply with the customer identification requirements, then the company may terminate the business relationship while at the same time it should examine whether it is warranted under the circumstances to submit a report of suspicious transactions/activities to the Authority.

4.5. Transaction and products that favor anonymity

The company must pay special attention to any money laundering or terrorist financing threat or risk that may arise from products or transactions that might favor anonymity, and take measures, if needed, to prevent their use for such purposes.

4.6. Construction of a customer' s business profile

Customer identification procedures and due diligence measures shall comprise the following:

(i) the identification and verification of the customer's identity on the basis of documents, data or information issued or obtained from a reliable and independent source;

(ii) the collection of information on the purpose and intended nature of the business relationship;

The company should establish to their satisfaction that they are dealing with a real person (natural or legal) and obtain sufficient evidence of identity to establish that a prospective customer is who he/she claims to be. The verification procedures necessary to establish the identity of the prospective customer should be based on reliable data, documents and information issued or obtained from independent reliable sources, i.e. those data, documents and information that are the most difficult to amend or obtain illicitly. The company should verify the identity of the beneficial owners and, for legal persons, they should obtain adequate information, data and documentation issued by independent and reliable sources so as to understand the ownership and control structure of the customer.

4.7. Specific customer identification issues

4.7.1. Natural persons

The Company ascertains the true identity of natural persons by obtaining the following information:

- True name and/or names used as these are stated on the official identification card or passport
- Full permanent address
- Telephone (home and mobile) and fax numbers
- Email address (if any)
- Date and place of birth
- Nationality

Specific requirements can be found in Appendix 3, attached to this manual.

4.7.2. Legal persons

The Company takes all necessary measures for the full ascertainment of the legal person's control and ownership structure as well as the verification of the identity of the natural persons who are the beneficial owners and exercise control over the legal person.

The verification of the identification of a legal person that requests the establishment of a business relationship or the execution of an occasional transaction, comprises the ascertainment of the following:

- The registered number
- The registered corporate name and trading name used

- The full addresses of the registered office and the head offices
- The telephone numbers, fax numbers and email address
- The members of the board of directors
- The individuals that are duly authorized to operate the account and to act on behalf of the legal person
- The beneficial owners of the private companies and public companies that are not listed in a regulated market
- The registered shareholders that act as nominees of the beneficial owners

Specific requirements can be found in Appendix 4, attached to this manual

4.8. Procedures for high risk customers

4.8.1. Customer identification and due diligence on a risk sensitive basis

The Company applies enhanced and additional customer due diligence measures in all instances which due to their nature entail a higher risk of money laundering or terrorist financing.

In order to determine what constitutes sufficient customer identification, one should take into account each customer's perceived risk associated with money laundering and terrorist financing. The extent and the number of checks that must be carried out for customer identification may vary depending on the perceived risk of the customer's country of origin or the type of service, product or account requested by the customer, or the customer's background and professional or business activities as well as the level of the expected turnover and transactions or the complexity of the customer's ownership structure. Information on the source of funds, i.e. how payments will be made, from where and by whom should be recorded so as to facilitate future transaction checks.

However, for high risk customers, the company takes additional measures for verifying their customers' identity, creating their business profile and ascertaining the source of assets i.e. how they have been acquired and their origin as well as monitor the movement of their transactions on a regular basis. In the cases where there is an accumulation of high risk customers and particularly when complex structures are combined with introduced business, enhanced due diligence measures should entail a direct contact with the natural person who ultimately owns or exercise control over the customer.

4.8.2. On-going monitoring of accounts and transactions

The Company (where applicable) should conduct ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with data and information maintained in respect of the customer, as well as ensuring that the documents, data or information held are kept up-to-date. The procedures and intensity of monitoring accounts and examining transactions should be risk sensitive.

5. RECORD KEEPING PROCEDURES

5.1. Record Keeping

The company keeps records of the documents/data for a period of 5 years, after the termination of the business relationship. It is provided that the documents/data relevant to ongoing investigations are kept until the Authority confirms that the investigation has been completed and the case has been closed.

5.2. Format of records:

The retention of the documentation and data (either original documents or certified true copies) are kept in electronic form and are easily retrievable in order to present them to any official regulatory authority after a request.

6. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

6.1. Introduction

Although it is difficult to comprehensively define a suspicious transaction, as the types of transactions which may be used by criminals who are involved in money laundering and terrorist financing are almost unlimited, a suspicious transaction will often be one which is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of account. It is, therefore, imperative to ensure that adequate information is maintained and to know enough about the customers' business in order to recognize that a transaction or a series of transactions is unusual or suspicious.

6.2. Internal reporting suspicious transactions and activities

Any person who knows or reasonably suspects that another person is engaged in money laundering or financing of terrorism offences, must report this information, as soon as is reasonably practical, after it comes to his/her attention.

7. EDUCATION AND TRAINING OF EMPLOYEES

Employees of the Company can be liable for failure to report information or suspicion, regarding money laundering and terrorist financing.

Therefore the employees are required to cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to money laundering or terrorist financing.

Employees' education and training program

The company ensures that its employees are fully aware of their legal obligations, by introducing a complete employee's education and training program.

The timing and content of the training program is adjusted according to the needs of the company. The frequency of the training can vary depending on the amendments of the legal and regulatory requirements and employees duties.

The training program aims at educating the employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trending used for this purpose.

Luiz Sanchez, Director

8. APPENDICES

APPENDIX 1

INTERNAL MONEY LAUNDERING SUSPICION REPORT

REPORTER

Name: .....Tel .....

Dept. .....Fax .....

Position.....E-mail.....

CUSTOMER

Name: ....

Address:..... .....

.....Date of birth .....

Contact/Tel/Fax/E-mail .....Occupation/Employer .....

.....Details on employer: .....

Passport No .....Nationality .....

ID Card No .....Other ID .....

INFORMATION/SUSPICION

Brief description of activities/transaction..... .....

....

....

Reason(s) for suspicion ....

....

....

REPORTER'S SIGNATURE.....**Date** .....

FOR MONEY LAUNDERING COMPLIANCE OFFICER'S USE

Date received.....Time received ..... Ref.....

Authority for Combating Money laundering Advised? Yes/No Date ..... Ref

APPENDIX 2

MONEY LAUNDERING COMPLIANCE OFFICER'S

INTERNAL EVALUATION REPORT

Reference..... Customer.....

Reporter..... Branch/Dept.....

ENQUIRIES UNDERTAKEN (Brief description)

.....

.....

.....

DOCUMENTS RESEARCHED/ATTACHED

.....

.....

.....

DECISION OF THE MLCO

.....

.....

.....

FILE REFERENCE.....

MONEY LAUNDERING
COMPLIANCE OFFICER'S Signature ..... ……Date.....

APPENDIX 3

List of identification documents for Individual:

- ✓ Original valid passport or identity card

- ✓ Original utility bill / bank statement (as verification of residential address not more than 6 months) **OR** in cases of Russian / CIS citizens then internal passport stating their residential address

Note: The Company takes copies of the originals presented and keeps copies of the pages containing all relevant information which are certified as true copies of the original documents.

List of additional information:

- ✓ Professional Resume (CV)
- ✓ Business background
- ✓ Source of wealth and source of funds

APPENDIX 4

List of identification documents for companies:

Legal documents:

- ✓ Copies of the Constitutional Documents
  - Certificate of Incorporation
  - Certificate of Directors and Secretary (where applicable)
  - Certificate of Shareholders
  - Certificate of Registered address
  - Memorandum and Articles of Association
  - Certificate of good standing for companies registered more than one year ago

The above documents may vary according to the relevant jurisdiction where the company is registered.

Additional information

- ✓ Copy of the legal ownership structure identifying the ultimate beneficial owner
- ✓ Copy of the trust deed /s duly signed by both related parties (nominee shareholder/s and ultimate beneficial owner/s)
- ✓ Resolution of the board of directors of the legal person for the opening of the account and granting authority to those who will operate it.
- ✓ Physical business address

For the physical persons related to the company the below are required:

- ✓ Valid passport copy or identity card
- ✓ Utility bill / bank statement (as verification of residential address not more than 6 months) **OR** in cases of Russian / CIS citizens then copy of their internal passport stating their residential address

Additional information for the companies Ultimate Beneficial Owner:

- ✓ Business Background
- ✓ Professional Resume
- ✓ Source of wealth and source of funds

For each corporate officer related to the company (in cases where this is applicable) the below are applicable:

- ✓ Copies of the Constitutional Documents (Depending on which Jurisdictions i.e. Certificates of Incorporation & Shareholders, Directors & Secretary – where this is applicable, registered address, Memorandum & Articles, Certificate of Good Standing for companies registered over 1 year) Copy of the Corporate structure identifying the ultimate beneficial owner
- ✓ Copy of the Corporate structure identifying the ultimate beneficial owner (applicable for complex corporate structures)