CRESCENT FINSTOCK LTD.

MONEY LAUNDERING DETERRENCE PROGRAMME AND ANTI MONEY LAUNDERING POLICY & PROCEDURES

Policy

This policy is to comply with high standards of Anti Money Laundering for practice in all markets. Crescent Finstock Ltd. (hereinafter referred to as "Company") has put in place this Money Laundering Deterrence Programme and Anti Money Laundering Policy & Procedures (hereinafter referred to as the "AML Policy & Procedures") which applies not only to money laundering, but also to terrorist financing. All references to money laundering and Anti Money Laundering in this Policy, Company Policies and Procedures and other supporting Anti Money Laundering policy, standards and local procedures includes terrorist financing where appropriate.

The Company will comply with all the specific provisions and the spirit of all relevant laws and regulations in relation to Anti Money Laundering and the Company Policies & Procedures. To these end the company will:

- Maintain appropriate operational controls;
- Undertake appropriate customer due diligence by:-
  - ❖ Identifying customers (and in case of non-individual clients the actual beneficial owners) and any other relevant party (hereafter referred to collectively as "customers") and verifying that identity, where required and
  - ❖ Obtaining additional know your customer information as appropriate and necessary.

- Take reasonable steps to enable recognition of suspicious transactions.
- Maintain procedures for identification of suspicious transactions and reporting of the validated suspicions to the appropriate authorities, as required;
- Co-operate with the regulatory authorities to the extent required by the applicable laws and provide information as may be required, without breaching the customer confidentiality agreement/understanding;
- Maintain appropriate records of customer identification and trail of transactions; and
- Give appropriate training to the relevant staff for effective implementation of the AML Policy & Procedures.

The Company AML Policies & Procedures should be read in conjunction with the guidance set out in the organizational Compliance Manual.

Objectives

The objectives of this Policy are to:

- Protect the reputation of the Company by taking all reasonable steps and exercising due diligence to deter the use of the Company / Company services by money launderers and those involved in criminal activities including the financing of terrorism.

- Protect the Company and its employees from unfounded allegations of facilitating money laundering and terrorist financing; and

- Avoid criminal, civil and regulatory sanctions which might result from unwitting involvement in money laundering and terrorist financing or from failure in operational controls.

Scope

The Policy sets minimum standards and applies to all staff and businesses of the Company. The Policy covers money laundering related to the proceeds of any crime and the financing of terrorism.

Operational Controls – Line Management Responsibility

Line management is responsible for ensuring that staff and businesses of the Company comply with the Company Policies & Procedures and standards as well as local Anti Money Laundering legislation and regulation including the Prevention of Money Laundering Act, 2002 and Securities and Exchange Board of India (hereinafter referred to as the "SEBI") Guidelines on Anti Money Laundering Standards. The role of the Company's Compliance function is to assist line management in meeting their responsibilities. All managers are urged to follow the advice and guidance provided by Officers of this function. The role and responsibilities of these officers are set out in the Compliance Manual.

The Principal / Compliance Officer with money laundering deterrence responsibilities have unrestricted access to Company Offices and Company Systems and records in order to carry out their responsibilities.

Operational controls – Customer Due Diligence

In general, before doing business with any prospective customer, appropriate customer due diligence should be undertaken and recorded. The customer due diligence process comprises (a) the identification and appropriate verification of identity and (b) additional Know Your Client information.

Know Your Clients Forms should be obtained in respect of all new customers and, where appropriate, in respect of existing customers on an ongoing basis. The extent to which Know Your Clients should be conducted should be determined on a risk based approach.

Customers treated as high risk for any reason should be the subject of enhanced Customer Due Diligence.

In certain limited circumstances and if within the overall framework of the SEBI guidelines, the company may apply reduced or simplified Customer Due Diligence measure for certain types of customers, products or transactions, taking into account all other risk factors. Any such reduced Customer Due Diligence procedures must be approved by the Principal / Compliance Officer.

Detailed procedures for Customer Due Diligence must be decided by the responsible Principal Officer, and be included in standard operating procedures covering any additional local legal and regulatory requirements, as may be applicable.

Customer Due Diligence

a. **Identification / Verification** - A prospective customer's identity should be obtained and verified using reliable, independent documentary and/or electronic source material. Where such evidence is not provided then the business should be declined.

   i. Where there are doubts about the quality or adequacy of previously obtained customer identification material for existing customers then, on the basis of materiality and risk, identification/verification should be carried out at appropriate times (e.g. immediately for high risk customers, when a transaction of significance takes place; when there is a material change in the way in which the account is operated; etc).

   ii. For non-personal customers (e.g. companies (particularly private companies), trusts, partnerships, etc) measure should be undertaken to understand the ownership and control structure (including the person/s who is/ are able to exercise control over the funds) and appropriate identification and verification undertaken.

   iii. Special care must be taken in respect of customers introduced by **intermediaries,** particularly where use is made of shell or shelf companies, trusts, nominee structures or other structures which appear to be established in order to hide the true ownership of assets. In all such circumstances the details of the identity and supporting identification material in respect of all relevant parties must be provided by the customer to the Company Office. The Company office remains responsible for ensuring that identification material and other Know Your Clients information meets Company and SEBI requirements. The acceptance of business introduced by or managed through any **intermediary** is subject to the relevant Company office undertaking appropriate and satisfactory initial and ongoing due diligence in respect of the **intermediary** and obtaining senior management authorisation. Approved relationships with **intermediaries** should be reviewed and re-approved on a regular basis.

   iv. As part of the due diligence measures sufficient information must be obtained in order to identify persons who beneficially own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and / or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. Beneficial ownership and control has to be identified; i.e. determine which

individual(s) ultimately own(s) or control(s) the customer and / or the person on whose behalf a transaction is being conducted.

v. Ongoing due diligence and scrutiny of transactions and trading account should be conducted.

b. Policy for acceptance of Customers - Company has developed customer acceptance policies and procedures which aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. The following safeguards are followed while accepting the customers.

i. No Trading account is opened in a fictitious / benami name, Suspended / Banned Organisation and person. Verification to be made from the data available from SEBI & Exchanges web link.

ii. Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to Customers' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover, etc and manner of making payment for transactions undertaken. These parameters enable classification of Customers into low, medium and high risk. Customers of special category (as given below) are classified under higher risk. Higher degree of due diligence and regular update of Know Your Clients profile are carried for these Customers.

- Non-Resident Clients
- High Networth Clients
- Trust, Charities, NGOs and organizations receiving donations
- Companies having close family shareholdings or beneficial ownership
- Politically exposed person (PEP). Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, senior politicians, senior government / judicial / military officers, senior executives of state-owned corporations, important political party officials etc. The norms applicable to PEP shall also be applied to the accounts of the family members or close relatives of PEPs,
- Companies offering foreign exchange offerings,
- Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, where there is unusual banking secrecy), Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent,
- Non face to face clients,
- Clients with dubious reputation as per public information available etc.

iii. It should be specified in what manner the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity / value and other appropriate details. Further the rights and responsibilities of both the persons (i.e. the agent-client registered with Company).

iv. Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement/ regulatory agency.

v. Before accepting any person as new client, it is ensured that the name/s of the proposed customer does not appear in the updated list of individuals and entities which are subject to various sanction measures such as freezing of assets / accounts, denial of financial services etc. as approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) accessed from the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. Also the same is verified from www.watchoutinvestors.com.

c. Know your Customer information

i. Know Your Clients Form information should be obtained prior to commencing the relationship and should be updated on a regular basis during the course of the business relationship. A risk based approach should be applied depending on the type of customer, nature of the business relationship, product and any other risk factor that may be relevant, as well as any specific local requirements.

ii. The client should be identified by the Company by using reliable sources including documents/ information. Adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship should be obtained by the Company.

iii. The information to be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the Company in compliance with the SEBI Guidelines. Each original document should be seen prior to acceptance of a copy and all copies of the documents should be self certified by the customer. Additionally information that can be verified from the government sites like income tax, etc would be verified from there to check the authenticity of the information given by the client.

d. Identification / Verification Measures - Where a potential client has not dealt with the Company in the past and wishes to open a trading account, the procedure is as under:

i. The client provides the necessary information required, including relevant documents

ii. The client account opening form / client registration form is duly completed by the client / clients nominee / dealer / sales executive.

iii. The member client agreement is executed (together with the Risk Disclosure Document) and the client registration form is duly filled and signed.

iv. All material amendments or alterations to client data (e.g. financial information or standing instructions) are done only after receipt of written request from the clients.

v. Following documents are to be collected for Non Individuals

1. Member and Client Agreement
2. Non Individual Client Registration Form
3. Risk Disclosure Document
4. All other supporting documents for identity / address of the non individual entity and residence and identity of the authorized signatory.
5. In case of companies, Board Resolution authorizing the directors / senior employees / authorized signatory to operate on behalf of the company. In case of other entities similar documents as required would be taken.

vi. Following documents are to be collected for Individuals

1. Member and Client Agreement
2. Individual Client Registration Form
3. Risk Disclosure Document
4. All other supporting documents for identity and residence of the individual.

Note: Photo proofs for identification of the client to be verified against originals and taken before opening a trading account with a new individual client. In case of non individual client, photo identities of the directors / authorised persons are to be verified against original and taken on record.

Know Your Clients information includes but is not limited to appropriate personal, business and financial details with regard to the customer, details on the purpose and intended nature of the business relationship including anticipated transactional activity, details as to the source of funds/wealth.

vii. The Unique client code (UCC) will be given to the non-institutional client only after receiving the form duly filled and signed, is in place.

viii. The information on the new client will be given to the Operations persons who will only open the account & allot UCC code to the client & register the same with exchanges.

e. Risk Profiling of Customers

i. Customer's acceptance to the potential money laundering risk associated to it. Based on the risk assessment, customers should be grouped into the following three categories viz:
   1. Low Risk
   2. Medium Risk
   3. High Risk

ii. All customers should be assigned one of these categories.

iii. The category of risk assigned to an account/customer will determine the applicable Customer Identification Procedures, subsequent monitoring & risk management.

iv. Customers who may pose a particular risk to the Company and Money Laundering Deterrence Programme and the Company's reputation, and who should normally be treated as high risk and subject to enhanced Customer Due Diligence, include, but are not limited to the following:-

- Members of the Company must not establish accounts or relationships involving unregulated money service businesses or unregulated businesses involved in aiming / gambling activities.

- Offshore Trusts, Special purpose Vehicles, International Business Companies which are established in locations with strict bank secrecy or confidentiality rules, or other legislation that may impede the application of prudent money laundering controls.

- Private companies, or public companies not subject to regulatory disclosure requirements, that are constituted in full or in part by bearer shares

- Customers with complex account relationships – e.g. multiple accounts in one, customers with high value and/ or high frequency transactional behavior.

- No account should be opened in anonymous or fictitious/benami name(s) i.e. to say the anonymous or fictitious/benami customers shall not be accepted.

- No account should be opened or transactions conducted in the name of or on behalf of banned/suspended individuals organizations, entities etc. for the purpose, necessary cross checks must be made to ensure the identify of a customer does not match with any person with criminal background or with banned/ suspended entities.

- No account should be opened if appropriate due diligence measures cannot be applied to a customer for want of verification documents on account of non co-operation of the customer or non-reliability of the data/information furnished of the Company.

Unless appropriate controls can be introduced to manage the risks posed by the above, then the business should normally be declined.

f. Non Face to Face Businesses Members of the Company should apply Customer Due Diligence procedures which ensure that the process is equally as effective for non face to face customers as for face to face customers. Financial services and products are now frequently provided to non face to face customers via postal, telephone and electronic facilities including the Internet. Customer identification procedures in these circumstances should include appropriate measure to mitigate the risks posed by non face to face business. Ongoing due diligence and scrutiny of transactions and trading account should be conducted.

g. Correspondent Accounts The Company is not permitted to open or maintain "payable through accounts", (being correspondent accounts that are used directly to transact business on their own behalf) without the written and ongoing annual approval of the Head of Compliance.

Operational Controls – Identification of Suspicious Transactions / Activity

The Company should ensure that appropriate scrutiny and monitoring of transactions, account activity and customers are undertaken in order to identify unusual and potentially suspicious activity.

Monitoring of transactions and account activity should be undertaken applying a risk based approach and having regard to the size and nature of the Company's business. In certain low risk, low volume businesses, manual monitoring may be appropriate. In other businesses systems generated. Anti Money Laundering exception reports or dedicated Anti Money Laundering automated monitoring systems may be required.

Transactions and account activity involving customers categorized as high risk should be subject to enhanced monitoring.

Examples of deemed to be suspicious transactions are:

- Cash transaction with Customers.
- Transactions in securities could be considered as suspicious if they are far away from the prevailing market price or theoretical market price without satisfactory explanations.
- Unusual Transactions by Clients of Suspicious Category (CSC).
- Transactions in securities could be considered as suspicious if they are far away from the prevailing market price or theoretical market price and are accompanied with offsetting transactions without satisfactory explanations.
- Transactions of a client would be considered as suspicious if the client does not confirm the transactions, does not sign the contract notes, ledger account confirmations, securities ledger confirmations or does not effect receipts or payments of moneys due for a considerably long period of time without satisfactory explanations.

- ❖ Customers with no discernible reason for using Company's service e.g. clients with distant addresses who could find the same service nearer home, client requirements not in the normal pattern of Company's business which could more easily be serviced locally.

- ❖ "cold calls" by investors who are not known personally by the staff member or the market in general.

- ❖ Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active, or the investor's business.

- ❖ Buying and selling of securities with no discernible purpose or in unusual circumstances e.g. churning at the client's request.

- ❖ Large quantity / frequently Buying & Selling in scrips categorized in Trade for Trade by the Exchange.

- ❖ Large numbers of transactions by the same counter party in small amounts of the same security, each purchased and then sold in 1 transaction, the proceeds being credited to an account different from the original account.

- ❖ Transactions where the nature, size or frequency appears unusual.

- ❖ Transactions not in keeping with normal practice in the market to which it relates, i.e. which reference to market size and frequency, or at off market prices.

- ❖ Customers whose identity verification seems difficult or Customers appears not to cooperate.

- ❖ Asset Management services for Customers where the source of the funds is not clear or not in keeping with Customers apparent standing / business activity.

- ❖ Substantial increases in business without apparent cause;

Operational Controls – Reporting of Suspicious Transactions

Every business unit in the Company must have procedures in place so that:

Any transactions and / or activities which are believed to be suspicious are reported to a central point (usually the Compliance / Principal Officer where the suspicious transactions and/or activities will be validated.)

- Principal Officer of Company would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions.
- The customer's account/s is/are reviewed in conjunction with the Principal / Compliance Officer and a decision made as to whether it should be closed.
- All significant exceptions are reported to the relevant Principal / Compliance Officer.

Operational Controls – Action to be taken on Reported Suspicious Transactions

All reported suspicious transactions of any customer or any customers with suspicious identity should be reviewed by the Principal / Compliance Officer thoroughly. After thorough verification & confirmation of transaction with suspicious in nature, the same should be immediately (not later than 7 days) reported to FIU, Ministry of Finance, New Delhi in writing.

Where the Company or an employee is put on notice that a particular customer or a particular type of transaction should be treated with caution, then it may be necessary to review the accounts or transactions in question, for example:

- When a transaction for a customer is identified as being suspicious, other transactions for that customer should be reviewed.

- When a customer's activities on one account have been identified as suspicious the customer's other related accounts should be examined.

In cases where it appears, or it is strongly suspected, that an account is being used for criminal purposes, it should be duly scrutinized and once concluded and found to be for criminal purpose would be closed, subject to any views by the authorities and to any local legal or regulatory constraints.

Where the customer is the subject of more than one validated suspicious transaction / activity/ report, then serious consideration should be given to closure of the relevant account/s and any other connected accounts. This decision should be reached by senior line and Compliance management.

Operational Controls – Co-operation with the Authorities.

It is Company policy to co-operate with the Anti Money Laundering authorities wherever possible, including complying with any requirements for reporting suspicious transactions / activity. However, due regard must be paid to the Company's duty of confidentiality to its customers. Confidential information about customers may, therefore, only be given to the authorities when there is a legal obligation to do so.

Customers must never be informed that a suspicion report has been made about them or that the authorities are interested in their activities. If such information were passed to a customer it could seriously hamper the enquiries of the authorities and may constitute the criminal offence of "tipping off". Care must be exercised when additional Customer Due Diligence is required to support the reason and purpose of any transaction / activity that may be considered unusual.

There may be occasions when the authorities ask for a suspect account to be allowed to continue to operate while they progress with their enquiries. In such cases the Company would wish to co-operate as far as is possible within the bounds of commercial prudence. Senior line and Compliance managers must always be made aware of instances of this nature.

Operational Controls – Maintaining Records

Adequate records should be maintained to enable the Company to demonstrate that appropriate initial and ongoing Customer Due Diligence (identification and Know Your Clients) procedures have been followed. These records should be maintained for a period as required in related act/law after the relationship has ended or such periods as may be required in terms of company policies & procedures or any local regulations, whichever is longer.

Adequate records of all transactions should be maintained in order to support reconstruction of transactions including the amounts, types of currency involved, if any, the origin of funds received into customer's accounts and the beneficiaries of payments out of customers' accounts. These records should be maintained for a period as required in related act/law after the date of the transaction.

In situations where the records relate to on-going investigations or transactions, which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

Records should be maintained of:

- All reports to the authorities and information provided to them;
- The results of any monitoring, which is carried out. These records should be maintained as per requirement in related act/law after closure of the case or such periods as may be required in terms of Company Policies & Procedures or any local regulations, whichever is longer.

All records should be readily retrievable

Internal Audit of the company operations regarding the compliance with the various regulatory requirements as per SEBI & AML regulations should be carried out periodically.

Operational Controls – Company Standards

The Company has established a number of minimum standards in relation to Anti Money Laundering controls for certain types of businesses and customers. The Company is required to apply these minimum standards as appropriate when undertaking activities or accepting the type of customers covered by any of these standards.

Operational Controls – Training

All new staff including temporary or contract staff who may be involved in customer business must receive suitable and timely induction training to ensure that they understand the Company's approach to money laundering deterrence, including:

- What money laundering is?

- The Company's requirements under the Policy, Company Policies & Procedures and additional policy and standards issued under the Company's Money Laundering Deterrence Programme, as appropriate.

- Legal or regulatory requirements and the risk of sanctions for themselves, the Company.
- Reporting requirements as prescribed by SEBI.
- The role played by their Principal / Compliance Officer in money laundering deterrence.
- The need to protect the Company's reputation.

Staff in high-risk areas should receive appropriate training to enable them to understand the money laundering techniques which are likely to be used in there area, and to remind them of their personal responsibilities under the Policy, Company Policies & Procedures and legal requirements.

Refresher training should be provided as appropriate and should as a minimum remind staff in high-risk areas annually of their responsibilities and alert them to any amendments to the Company's Money Laundering Deterrence Programme or local legal and / or regulatory requirements, as well as any new money laundering techniques being used.

Operational Controls – Monitoring and Review of the Company's Money Laundering Deterrence Programme.

Regular monitoring must be undertaken by line management and / or Compliance to check that all businesses are complying with the Company Policies & Procedures and local legal and regulatory requirements as prescribed under the PMLA and by SEBI.

Operational and functional review work will be undertaken by Compliance and / or Audit functions, as appropriate. Compliance Officers will liaise with their relevant Audit function to agree appropriate review programmes and responsibility for review work.

The level and frequency of monitoring and review work will be undertaken having regard to materiality and risk in relation to the business and customer base.

Further information

Any queries or problems concerning the Policy, the Company Policies & Procedures or legal requirements relating to money laundering should be referred to the Principal / Compliance Officer of the Company