ANTI MONEY LAUNDERING POLICY & PROCEDURES

GCM SECURITIES LIMITED

1. Introduction

Parliament of India enacted Prevention of Money Laundering Act, 2002 (PMLA) to prevent money-laundering and to provide for confiscation of property derived from, or involved in, money-laundering and for matters connected therewith or incidental thereto. The provisions of PMLA came into force on 01st July 2005. Section 12 of PMLA, inter-alia, requires all intermediaries associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 to maintain a record of all transactions, the nature and value of which has been prescribed under the rules notified under the PMLA. Pursuant to this, Securities and Exchange Board of India (SEBI) issued Guidelines on Anti Money Laundering Standards and various circulars from time to time to implement the provisions of PMLA in the securities market and to prevent and impede money-laundering and combat financing of terrorism. GCM Securities Ltd Ltd (hereinafter referred to as 'GCM' or 'the Company'), hereby adopts and bring into effect this **Anti Money Laundering Policy & Procedures** (AML Policy & Procedures) in accordance with the provisions of PMLA and the rules made thereunder, SEBI Guidelines and Circulars issued from time to time on this subject. The policy applies not only to money laundering, but also to terrorist financing. All references to money-laundering in this policy, company policies and procedures and standards include terrorist financing as appropriate.

2. Policy

The Company shall endeavor at all times to comply, in letter and spirit, with the provisions of all relevant laws, rules, regulations, guidelines and circulars issued by regulatory authorities in relation to anti-money laundering and the Company's policies & procedures. To these ends the Company shall:

- Appoint a Principal Officer responsible for ensuring compliance with the PMLA;
- Appoint a Designated Director as defined in Rule 2 (ba) of the PML Rules, who should be responsible for ensuring the compliance with the PMLA requirements;
  "Designated Director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes the Managing Director or a Whole-time Director duly authorized by the Board of Directors. The appointment details of the Designated Director such as, name, designation, etc should be communicated to the Office of the Director, FIU-IND and update the same on the FIU website and intimate in future whenever there is any change.
- Establish appropriate 'Customer Due Diligence Process' for:
  - identification of clients (and actual beneficial owners) and verification of their identity;
  - obtaining additional 'know your client' information as appropriate and necessary;
  - acceptance of clients;
  - identification of suspicious transactions and reporting of the validated suspicions to the appropriate authorities, as required;
- Maintain appropriate records of customer identification and trail of transactions; and
- 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;
- 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 / GCM Compliance Manual.

3. Objectives

The objectives of this Policy are to:

- Prevent and deter the use of the Company/Company's services by money launderers or those involved in criminal activities including financing of terrorism and to protect the reputation of the Company.
- Protect the Company and its employees against unfounded allegations of facilitating money laundering and terrorist financing; and
- Protect the Company and its employees against any criminal, civil and regulatory actions which might result from inadvertent involvement in money laundering and/or terrorist financing or from failure in operational controls.

4. Scope

The Policy sets minimum standards and applies to all staff and business activities of the Company.

5. Responsibility of Principal Officer & Line Management

The Company shall appoint a Principal Officer, who shall be responsible for ensuring compliance with the provisions of the PMLA and this AML Policy & Procedures. The Company shall immediately intimate the name, designation, address including email address of the Principal Officer to the Office of the Director-FIU, 6th Floor, Hotel Samrat, Chanakyapuri, New-Delhi – 110021. Any change in the particulars of Principal Officer shall also be immediately intimated to the Office of the Director-FIU.

From operations standpoint, it is the responsibility of Company's line management to ensure that their respective departments and staff are complying with the Company's AML Policy & Procedures and local anti-money laundering legislations, standards and guidelines laundering. The role of Company's Principal Officer is to guide, advise and assist the line management in fulfilling their responsibilities in relation to anti-money. Further, the Principal Officer shall be assisted by the Compliance Department in discharging his responsibilities towards ensuring compliance with the provisions of the PMLA and this AML Policy & Procedures. The Principal Officer shall have unrestricted access to the Company's Offices, IT Systems and records in order to carry out his responsibilities.

The Principal officer is also responsible for reviewing the alerts received from exchange / DP and has to follow proper methodology of enquiring into the alert. He will find about the details regarding the transaction and without informing the client about the alert will collate various information in support of the trade to reach to a conclusion whether the trade is required to be reported to the FIU. He is required to maintain the alerts with his conclusion regarding the same. In case if the transaction is required to be reported then he should inform the same to FIU and the Exchange / CDSL as required.

6. Customer Due Diligence Process

The Company shall put in place appropriate customer due diligence measures, which should be applied to all customers (new as well as existing). These measures comprise,

(a) Procedure for Identification and Verification of Customers:

(i) Before admitting any person as a customer, the Company shall obtain sufficient information in order to identify the customer and any other person(s) with whom lies the beneficial ownership or ultimate control. The same should be done for all the existing customers as well. This should be done by obtaining 'Know Your Customer' (KYC) information.

(ii) KYC information should be updated on a regular basis during the course of business relationship.

(iii) The customer should be identified by the Company using documents/information from reliable sources. Adequate information to satisfactorily establish the identity of each client and the purpose of the intended nature of the relationship should be obtained by the Company.

(iv) The procedure to be followed for admitting a person as a client is as under:

- Client/Client's Nominee/Company's Sales Executive should submit the account opening form/ client registration form duly filled-in and signed by the prospective client.
- The Member-Client Agreement should be executed together with the Risk Disclosure Document.

- The Client should provide all the necessary information required alongwith the relevant documents. Following documents should be collected from non-individuals clients:
    1. Non-individual Client Registration Form;
    2. Member and Client Agreement;
    3. Risk Disclosure Document;
    4. All other supporting documents for identity/address of the non individual entity and the authorized signatory;
    5. In case of companies, board resolution authorizing the directors/senior employees/ authorized signatory to operate on behalf of the company and to deal in the derivative market. In case of other entities, similar documents would be required;
    6. PAN Card copy of Non-individual client and all the partners/directors in case the client is a partnership firm or body corporate;
    7. Bank Account proof.
- Following documents are to be collected from individual clients:
    1. Individual Client Registration Form;
    2. Member and Client Agreement;
    3. Risk Disclosure Document;
    4. All other supporting documents for identity and residence of the individual;
    5. PAN Card copy;
    6. Bank Account proof.
- Photo identity proof of client should be verified against originals. In case of a non-individual client, photo identities of the directors/authorized persons should be verified against originals and taken on record.
- If all the documents and form are in order, client should be allotted a Unique Client Code (UCC).
- Clients can start transacting only after they have been allotted UCC.

The above specified documents having annual changes should be collected from clients annually and in case of documents where any change has happened then the same should be collected as and when the change happens. Other documents should be collected once in 5 years as felt necessary by the compliance officer.

(v) Prospective customer's identity should be verified using reliable, independent documentary and/or electronic source material. Where such evidence is not available the business should be declined.

(vi) For information to be adequate enough to satisfy competent 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 photocopy and all photocopies of the documents should be self-certified by the customer. Additionally, information that can be verified from the government websites like income tax etc. should be verified accordingly to establish the authenticity of the information given by the client.

(vii) Where there are doubts about the quality or adequacy of previously obtained customer identification information for the existing customers then, on the basis of materiality and risk

category of each client, identification/verification should be carried out at appropriate time (i.e. immediately - for high risk customers, immediately - when a transaction of significance takes place, immediately - when there is a material change in the way in which the account is operated etc.).

(viii) For non-individual customers e.g. companies (particularly private companies), trusts, partnerships, etc. measures 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 should be done.

(ix) 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 and verified using client identification and verification procedures as early as possible. 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(s) is/are being conducted & includes person who exercises ultimate effective control over a legal person or arrangement.

For determining Beneficial Ownership, following approach is followed as specified in SEBI circular No. CIR/MIRSD/2013 dated 24th January 2013:

- For clients **other than individuals or trusts:**

  Where the client is a person *other than an individual or trust*, viz., company, partnership or unincorporated association/body of individuals, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

  a. The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest. Explanation: Controlling ownership interest means ownership of/entitlement to:
     i. more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;
     ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
     iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

  b. In cases where there exists doubt under clause 4 (a) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means. Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

c. Where no natural person is identified under clauses 4 (a) or 4 (b) above, the identity of the relevant natural person who holds the position of senior managing official.

- **For client which is a trust:**
  a Where the client is a *trust*, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.
- **Exemption in case of listed companies:**
  a Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.
- **Applicability for foreign investors:**
  a Intermediaries dealing with foreign investors' viz., Foreign Institutional Investors, Sub Accounts and Qualified Foreign Investors, may be guided by the clarifications issued vide SEBI circular CIR/MIRSD/11/2012 dated September 5, 2012, for the purpose of identification of beneficial ownership of the client.

For independent identification of the person in the course of Customer Due Diligence the documents to be taken regarding the identity proof of the designated / responsible person and additionally the proof of residence would be taken. The proofs to be taken would be as prescribed by the regulators and as specified above.

(x) Before opening an account it must be ensured that the identity of the prospective client does not match with a person having known criminal background and that there are no prohibitory orders/sanctions against the prospective client by any enforcement/ regulatory agency.

(xi) Before accepting any person as a client, it must be ensured that such person's name does not appear and is not linked in anyway to the individuals and entities listed in the consolidated list of individuals and entities maintained by Security Council Committee established pursuant to United Nations Security Council Resolution 1267 (1999). The consolidated list can be accessed from the UN website at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and http://www.un.org/sc/committees/1988/list.shtml. All existing accounts should be scrutinized to ensure that no account is held by or linked to any of the individuals or entities included in the aforesaid consolidated list. The Company shall intimate full details of accounts bearing resemblance to any of the individuals/entities in the aforesaid consolidated list to SEBI and FIU-IND.

(xii) It must be ensured that no account, existing or new, bear any resemblance to the designated individuals/entities mentioned in the Schedule to the Government of India (Ministry of Home Affairs – Internal Security-I Division) Order dated August 27, 2009 (as amended) under Unlawful Activities (Prevention) Act, 1967. The updated list of such designated individuals/entities would be

communicated by SEBI from time to time. In the event, particulars of any customer (s) match the particulars of designated individuals/entities listed in the said Schedule, the Company shall, within 24 hours, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer in its books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. Such particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in. The company shall also send the particulars of the communication mentioned above through post/fax and through e-mail (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051 as well as the UAPA nodal officer of the state/UT where the account is held, as the case may be, and to FIU-IND. In case the aforementioned details of any of the customers match the particulars of designated individuals/entities beyond doubt, the Company should prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in. The Company shall also file Suspicious Transactions Report (STR) with FIU-IND covering all transactions in such accounts, carried through or attempted, as per the prescribed format.

(xiii) Non Face-to-Face Customers: Company should apply Customer Due Diligence procedures ensuring that the process is equally effective for non face-to-face customers & face-to-face customers. Financial services and products are frequently provided to non face-to-face customers via telephone and electronic facilities including Internet. To mitigate the risks posed by such non face-to-face business, customer due diligence, scrutiny of transactions and trading account should be conducted on an ongoing basis.

(xiv) All material amendments or alterations to client information (e.g. financial information or standing instructions) should be effected only on receipt of written request from the clients.

(xv) Company shall determine if the existing or potential client is a Politically Exposed Person (PEP) by seeking additional information from clients, accessing publicly available information etc. If the existing/potential client is found to be PEP, approval should be obtained from the Whole-time Director of the Company to admit the PEP as client or to continue the existing business relationship. The Company shall also seek the details of source of funds of clients identified as PEP.

(xvi) A copy of client identification programme should be forwarded to Director, FIU-IND, New-Delhi.

(b) Risk Profiling of Customers

(i) Risk profiling of all customers should be done based on factors such as customer background, location, nature of business activity or transaction, trading turnover etc. This should be done by the Account Opening Team in consultation with the Principal Officer of the Company. Based on the risk assessment, customers should be grouped into the following three categories –

1. Low Risk – The clients having good income level, staying in an country recognized by FATF has a signatory country, clients with low volume, etc would be considered as less risky

2. Medium Risk – The clients who are found to be defaulting or not in compliance with any of the points specified above in the low risk category would be classified under medium risk
3. High Risk – Clients who are found to be defaulting in majority of the points specified in low risk or who are PEP classified would be classified as high risk and regular watch on their trading activity would be classified under high risk category

(ii) The Company shall apply customer due diligence measures to clients on a risk sensitive basis i.e. applicability of customer identification procedures, documentary requirements, ongoing account monitoring, transaction monitoring & risk management will depend on the risk profile of customer. Customers identified as high risk category shall be subjected to enhanced customer due diligence process. Conversely, a simplified due diligence process may be adopted for low risk categories of customers.

(iii) In certain limited circumstances, within the overall framework of the SEBI guidelines, the Company may apply reduced or simplified Customer Due Diligence measures for certain types of customers, products or transactions, taking into account all the risk factors. Any such reduced customer due diligence procedures must be approved by the Principal Officer.

(iv) Clients of Special Category (CSC): Customers who may pose a particular risk to the Company, to money laundering deterrence programme and to 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:

- 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 and which are constituted in full or in part by bearer shares
- Customers with complex account relationships e.g. multiple accounts in one
- Non-Resident Clients
- High Net-worth 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, etc. We shall also independently access and consider other publicly available information along with any other information which we may have access to.

- Non face to face clients
- Clients with dubious reputation as per public information available etc.

For clients other than as specified under Client of Special Category (CSC), we are defining risk categorization of clients in Low, Medium & High Risk based on their trading pattern, Financials etc & were reviewed periodically.

(c) Policy for Acceptance of Clients

The Company has developed customer acceptance policy 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. Staff should adhere to following safeguards while accepting customers:

- No Trading account should be opened in a fictitious/benami name or on an anonymous basis, or in the name of a suspended/banned entity.
- No Trading account should be opened in the name of any person with criminal background.
- Members of the Company must not establish accounts or relationships involving unregulated money service businesses or unregulated businesses involved in gambling activities.
- No account should be opened if appropriate due diligence measures cannot be applied to a customer for want of verification of documents or on account of non-cooperation of the customer or due to non-reliability of the data/information furnished by the customer.
- In case an account is being opened & operated by an agent on behalf of Principal, 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).

(d) Reliance on Third Party for Client Due Diligence:

The Client Due Diligence & In-Person verification of the clients will be done by the staff of the Group / company, however in future if any support will be taken from any third party agency then the company will carry out various tests before passing on the responsibility to the third party as the company understands that the Reliance on the third party will be at their own risk and thus will authorize any third party to do the activity only after thorough due diligence has been done of that third party agency before appointing that third party agency.

(e) Continuous Monitoring of Transactions & Identification of Suspicious Transactions/Activities

(i) The Company shall undertake appropriate scrutiny and monitoring of customers' account activity and transactions on an ongoing basis in order to identify any unusual and potentially suspicious activity. This is possible only when the Company's staff has an understanding of the normal activity of the client so that they can identify any deviant transactions/activities;

(ii) Transactions and account activity involving customers categorized as high risk should be subject to enhanced monitoring. The monitoring of transaction will also be done on basis of Volume of trading done by the client in proportion to his financial details / networth as disclosed in the KYC. The financial details will also be updated on periodical basis to have a proper control on their transactions.

(iii) Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith –

a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
b) appears to be made in circumstances of unusual or unjustified complexity; or
c) appears to have no economic rationale or bonafide purpose;
d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Some of the circumstances which may lead to suspicion and certain transactions which are deemed to be suspicious in nature are:

- False identification documents or identification documents which could not be verified within reasonable time;
- Non-face to face clients;
- Doubt over the real beneficiary of the account;
- Accounts opened with names very close to other established business entities;
- Suspicious background or links with known criminals;
- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale;
- Unexplained transfers between multiple accounts with no rationale;
- Unusual activity compared to past transactions;
- Use of different accounts by client alternatively;
- Sudden activity in dormant accounts;
- Activity inconsistent with what would be expected from declared business;
- Account used for circular trading;
- Unusual or unjustified complexity in transactions;
- No economic rationale or bonafide purpose of transactions;
- Doubtful source of funds;
- Transfer of investment proceeds to a 3rd party;
- Transactions reflecting likely market manipulations;
- Suspicious off-market transactions;
- Transaction value just below threshold in an apparent attempt to avoid reporting;
- Large sums being transferred from overseas for making payments;
- Transactions inconsistent with the clients apparent financial standing;

- Inconsistency in the payment pattern by client;
- Block deal which is not at market price or prices appear to be artificially inflated/deflated;
- Cash transaction with customers;
- Unusual transactions by Clients of Special Category (CSC), businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export and import;
- 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 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 services e.g. clients with distant addresses who could find the same service nearer home or client's 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 or frequent buying & selling by clients in scrips categorized as 'Trade for Trade' by Exchange;
- Large numbers of transactions of small amounts by the same client in the same security, first purchased and then sold, the proceeds being credited to an account different from the original account;
- Transactions not in keeping with normal practice in the market to which it relates, i.e. with reference to market size and frequency or at off-market prices;

High degree of due diligence shall be applied in respect of clients of High Risk clients. The process of review of high risk clients will require detailed review at the time of opening of these accounts. Further the transaction of these Clients should be analysed and reviewed. Using various data analystic methods the company would also study the movement in the script in which the clients trade. In case of any modification to the information provided during account opening, the same should be thoroughly analysed and proper care to be taken to avoid any mis-happening. In case any suspicion is found in any activity of such account then the action should be taken to report the same as suspicious to the FIU and other regulators as required in law.

The KYC department should also enquire about the beneficiary information for various non-individual entities and also carry-out the verification process by enquiring for the Proof of Identity & Proof of Address of owners as indicated in the earlier part of the PMLA policy.

All the clients of the company will be continuously reviewed to check whether the client's name

not matches with names in any of the following lists:
- SEBI Debarred List
- UNSC
- PEP
- OFAC (Office of Foreign Access and Control given by US Treasury Dept.)
- Such other list that may be specified by the Regulators/Compliance Department from time to time.

Further for high risk clients this review will be done on a continuous manner on a weekly / monthly basis as may be decided by the management.

(iv) The compliance department of the Company shall randomly examine a selection of transactions undertaken by clients to examine and comment on whether or not they are in the nature of suspicious transactions.

7. Maintaining & Retaining Records

(i) The Company shall maintain adequate records so as to enable it to demonstrate that appropriate initial and ongoing Customer Due Diligence procedures have been followed. To this end, Company shall maintain records of

- Client Identification Procedure
- All documents collected at the time of client on-boarding
- Customer Risk Profiling
- Account Files
- Business Correspondences

(ii) Adequate records of all transactions should be maintained in order to permit reconstruction of transactions including the amounts, types of currency involved, the origin of funds received into customer's accounts and the beneficiaries of payments out of customer's accounts. To this end, the Company shall retain following information for the account of their customers in order to maintain a satisfactory audit trail:

a. the beneficial owner of the account;
b. the volume of the funds flowing through the account; and
c. for selected transactions:
   - the origin of the funds;
   - the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
   - the identity of the person undertaking the transaction;
   - the destination of the funds;
   - the form of instruction and authority.

(iii) The Company shall maintain record of following transactions as prescribed under Rule 3, notified under the PMLA:

a. all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;

b. all series of cash transactions integrally connected to each other which have been valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rs.10 lakh;
c. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
d. all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

For the above transactions, Company shall also maintain following information:

a. the nature of the transactions;
b. the amount of the transaction and the currency in which it is denominated;
c. the date on which the transaction was conducted; and
d. the parties to the transaction.

(iv) The Company shall maintain records of all the reports made to the authorities and information provided to them;

(v) The Company shall also maintain the results of any monitoring of transactions or account, which is carried out.

(vi) All records should be readily retrievable.

(vii) The Company shall maintain all the above records for a period of 5 years from the date of cessation of transactions between the Company and the client.

(viii) 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.

8. Reporting of Transactions including Suspicious Transactions

(i) All staff members shall ensure that any transaction and/or activity which is believed to be suspicious is reported to the Principal Officer who shall validate whether the transaction/activity is of suspicious nature or not. However, it should be ensured that there is no discontinuity in dealing with the client until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended or other action taken. Such customer's accounts should be reviewed in conjunction with the Principal Officer and a decision should be made as to whether it should be closed.

(ii) In some cases, customers may abandon transactions on being asked to give some additional details/documents/information. It is clarified that staff shall report all such attempted transactions in Suspicious Transactions Report, even if they are not executed by customers, irrespective of the amount of the transaction.

9. Action on Reported Suspicious Transactions & Cash Transactions

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

(ii) 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.

(iii) In cases where it appears, or it is strongly suspected, that an account is being used for criminal purposes, it should duly scrutinized and once confirmed, the Account should be closed, subject to any advice by the regulatory authorities.

(iv) Where a customer is subjected to 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 management, Compliance Officer and Principal Officer.

(v) Reporting to Financial Intelligence Unit – India (FIU-IND):
Principal Officer of the Company shall act as a central reference point in facilitating onward reporting of transactions to FIU-IND and for playing an active role in the identification and assessment of potentially suspicious transactions. Principal Officer of the Company shall submit Cash Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) as prescribed under Rule 3, notified under the PMLA to:

Director, FIU-IND, Financial
Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri, New-Delhi – 110021
http://fiuindia.gov.in/

and shall adhere to the following instructions given in SEBI Master Circular no. SEBI/ HO/ MIRSD/ DOP/ CIR/ P/ 2019/113 dated October 15, 2019 while reporting:

a. Cash Transaction Reports (CTRs):
   - The CTRs (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month;
   -

b. Suspicious Transaction Reports (STRs):

- All suspicious transactions shall be reported by the Principal Officer to Director, FIU-IND within 7 working days of establishment of suspicion at the level of Principal Officer. The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.

c. The Principal Officer will be responsible for timely submission of CTRs and STRs to FIU-IND;
d. Utmost confidentiality should be maintained in filing of CTRs and STRs to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.
e. No NIL reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

Every control system should be established in the organization to take care that the reporting of suspicious activity should be done to the regulators only and no client should be informed to the suspicious reporting being done about themselves or about anybody else. The Company and its staff are strictly required to ensure that there is no 'tipping-off' to any customers about any suspicious transaction reporting that has been made to the regulators. The organization may use the learning from the suspicious activity to train the staff for controlling any suspicious activity and use the information for investor / clients awareness about the suspicious transactions.

10. Co-operation with Authorities

(i) The Company and its staff shall cooperate with Anti Money Laundering authorities and shall comply with requirements for reporting any suspicious transactions/activity. However, due regard must be paid to the Company's policy of maintaining customer confidentiality. Confidential information about customers may, therefore, only be given to the authorities when there is a legal obligation to do so.

(ii) The Company and its staff shall strictly ensure that there is no 'tipping-off' to customers about suspicious transaction report being made about their transactions/activities or that the authorities are looking into their transactions/activities. If such information is passed to a customer, it may seriously hamper the enquiry/investigation of the authorities.

(iii) 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 cooperate with the authorities, as far as possible, within the bounds of commercial prudence and applicable laws. Senior line management and Principal/Compliance Officer must always be kept aware of such instances.

11. Hiring of Employees:

The company has a sufficient system of screening the employees before their appointment so that they are suitable and competent to perform their duties. The company would also carry out on going employee training programme so that the Employees are adequately trained in AML and CFT procedures as required.

The HR department will also be carrying out the background check of the employee being hired by calling the references provided by the employee or a third party verifier agency to carryout a proper check before employing the employee. The HR department will also try to get the creditability of the employee by talking to the previous employers and get their feedback of the senior / HR department / the department where the employee was working with his past employments.

12. Training

(i) All new staff, whether permanent, temporary or on contract, who may be involved in handling customers' on-boarding, execution of transactions must receive suitable induction training to ensure that they fully understand their responsibilities under the Company's AML Policy & Procedures. Such training shall inter-alia cover following topics:

- What is money-laundering?
- Company's requirements and obligations under the AML Policy & Procedures.
- Company's legal or regulatory requirements and the risk of sanctions/penalties for staff as well as the Company.
- Reporting requirements as prescribed by SEBI.
- The role played by Company's Principal/Compliance Officer in money laundering deterrence.
- The need to protect the Company's reputation.

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

(iii) Annual refresher training courses should be conducted for staff in high-risk areas to remind them of their responsibilities and alert them to any amendments to the Company's AML Policy & Procedures or local legal and/or regulatory requirements, as well as any new anti-money laundering techniques being used.

13. Investor Education

The company also intends to take effective steps for Investor Education regarding the PMLA regulations. Accordingly the KYC team of the company intends to Educate the Investor regarding the requirements of PMLA and will also call for various information like Income proof / DP holding / Networth, etc so as to understand the financial position of the client.

14. Procedure for freezing & unfreezing of funds, financial assets or economic resources or related services

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the prevention of, and coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government had issued an Order dated March 14, 2019 detailing the procedure for the implementation of Section 51A of the UAPA, in view of the reorganization of Divisions in the Ministry of

Home Affairs and allocation of work relating to countering of terror financing to the **Counter Terrorism and Counter Radicalization (CTCR)** Division. Under the aforementioned Section, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. The obligations to be followed by intermediaries to ensure the effective and expeditious implementation of said Order has been issued vide SEBI Master Circular ref. no: SEBI/ HO/ MIRSD/ DOP/ CIR/ P/ 2019/113 dated October 15, 2019, which needs to be complied with scrupulously. Accordingly, in order to ensure compliance with the Order the company shall follow the following procedure:

In case if any client is found to be guilty under the PMLA provisions then the following procedure to be followed by the Company, will be as under:

1) If the particulars of any of customer/s match the particulars of designated individuals/entities, the Company shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer on their books to the Joint Secretary (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The Company would also convey the information through e-mail at jsctcr-mha@gov.in.
2) The Company would inform the IS-I Division of MHA so that they may take effective action like informing the State Police and /or the Central Agencies for conducting the verification of the individuals/ entities identified by the registered intermediaries.
3) The Company to provide full support to the appointed agency for conducting of the verification so that the verification gets completed within a period of 5 working days.
4) The Company would not provide any prior notice to the designated individuals/entities.

Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

i. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to the broker. Broker shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of CTCR Division of MHA as per the contact details given above within two working days.

ii. The Joint Secretary (CTCR), MHA, being the nodal officer for (CTCR) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the broker. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of CTCR Division shall inform the applicant.

15. Monitoring and Review of the Company's AML Policy & Procedures

(i) The Company shall undertake regular monitoring of its operations through line management and/or Compliance to check that all businesses are complying with the Company's AML Policy & Procedures as well as local legal and regulatory requirements as prescribed under the PMLA and by SEBI.

(ii) Operational and functional review work shall be undertaken by Compliance and/or Audit functions, as appropriate. Compliance Officer shall liaise with their relevant Audit function counterpart to arrive at appropriate review programme and responsibility.

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

16. Further Information

Any queries or doubts concerning Company AML Policy & Procedures or any local legislation or regulation or Circulars or Guidelines relating to Anti Money Laundering and/or Combating Financing of Terrorism shall be referred to the Principal Officer of the Company.

17. Definitions:

- "Aadhaar number/ Aadhar" means an identification number as defined under sub-section (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;

- "Authentication" means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;

- "Resident" means an individual as defined under sub-section (v) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;

  "Identity information" means the information as defined in sub-section (n) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;

  "e – KYC authentication facility" means an authentication facility as defined in Aadhaar (Authentication) Regulations, 2016;

- "Yes / No authentication facility" means an authentication facility as defined in Aadhar (Authentication) Regulations, 2016;

Implementation of Aadhaar:

As per notification given by the Ministry Of Finance (Department of Revenue) dated 1st June, 2017 under Prevention of Money-laundering (Maintenance of Records) Second Amendment Rules, 2017, "Aadhaar" has become mandatory and we have a policy to collect Aadhaar number along with supporting documents from all the clients.

The organization is required to comply with important requirements as mentioned in the notification on two types of clients:

- Individual
- Other than Individual i.e.Entities

In case of Individual:

- The client shall submit to us the Aadhaar number issued by the Unique Identification Authority of India;

In case of other than Individual i.e. Entities:

- Client is a Company/Partnership firm/Trust/ Unincorporated association or body of individuals , shall submit to us certified copies of **Aadhaar Numbers;** Issued to managers, officers or employees in case of company and the person in case of partnership firm/trust/unincorporated association or a body of individuals holding an attorney to transact on behalf of the client entity.
- At the time of receipt of the Aadhaar number under provisions of this rule, shall carry out authentication using either e-KYC authentication facility or Yes/No authentication facility provided by Unique Identification Authority of India (UID).
- If the client does not submit the Aadhaar number, at the time of commencement of an account based relationship with M/s GCM Securities Ltd Ltd, then they submit the same within a period of six months from the date of the commencement of the account based relationship.
- For existing clients already having an account based relationship with reporting entities prior to date of this notification i.e. June 1, 2017, the client shall submit the Aadhaar number by December 31, 2017.
- If client fails to submit the Aadhaar number within the aforesaid time limits the said account shall cease to be operational till the time Aadhaar number is submitted by the client.
- In case the identity information relating to the Aadhaar number submitted by the client does not have current address of the client, the client shall submit an officially valid document to the M/s GCM Securities Ltd Ltd.

In view of the Supreme Court judgement dated 26.09.2018 regarding Aadhar Card not being mandatory for registration of clients in the Capital Market, the provision of the above point 17 is not applicable and hence the above point is no longer valid.

18. Other Points

- The Policy / documents in relation to CDD will be reviewed once in a year or as and when required and will be presented before the board in the board meeting.

- The company has made the PMLA policy which is informed to the Investors through the company's website and the company is also carrying out Investor Education initiative by explaining the investors about the PMLA rules & requirements.

****