'Know Your Customer' Guidelines

Anti Money Laundering Standards

1. Know Your Customer Standards

a) The objective of the KYC guidelines is to prevent brokers from being used, intentionally or unintentionally, by criminal elements for money laundering activities. KYC procedures enable brokers to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The revised KYC policy of the broker incorporates the following four elements:

- Customer Acceptance Policy (CAP)
- Customer Identification Procedures (CIP)
- Monitoring of Transactions; and
- Risk Management

b) A customer for the purpose of KYC Policy is defined as:

- A person or entity that maintains an account and/or has a business relationship with the broker.
- One on whose behalf the account is maintained (i.e., the beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors, etc as permitted under the law
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the broker, say, a wire transfer or issue of high value demand draft as a single transaction.

2. Customer Acceptance Policy (CAP)

a) The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in by the broker. The dealers shall accept customer strictly in accordance with the said policy:

- No account shall be opened in anonymous or fictitious/benami name(s)

- Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc., to enable categorization of customers into low, medium and high risk called Level I, Level II and Level III respectively; Customers requiring veryhigh level of monitoring e.g., Politically Exposed Persons (PEPs) may be categorized as Level IV.

- The dealers shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of AML Act, 2002 and guidelines issued by RBI from time to time.

- The dealers shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures i.e., branch is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of data/information furnished to the branch. The dealers shall, however, ensure that these measures do not lead to the harassment of the customer. However, in case the account is required to be closed on this ground, the dealers shall do so only after permission of Senior Official of their concerned Offices is obtained. Further, the customer should be given a prior notice of at least 20 days wherein reasons for closure of his account should also be mentioned.

- The dealers shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. RBI has been circulating lists of terrorist entities notified by the Government of India so that brokers exercise caution against any transaction detected with such entities. The dealers shall invariably consult such lists to ensure that prospective person/s or organizations desirous to establish relationship with the broker are not in any way involved in any unlawful activity and that they do not appear in such lists.

b) The dealers shall prepare a profile for each new customer based on risk categorization. The broker has devised a revised Composite Account Opening Form for recording and maintaining the profile of each new customer. Revised form is separate for Individuals, Partnership Firms, Corporate and other legal entities, etc. The nature and extent of due diligence shall depend on the risk perceived by the dealer. The dealers should continue to follow strictly the instructions issued by the broker regarding secrecy of customer information. The dealers should bear in mind that the adoption of customer acceptance policy and its implementation does not become too restrictive and should not result in denial of brokering services to general public, especially to those, who are financially or socially disadvantaged.

c) The risk to the customer shall be assigned on the following basis:

⇒ **Low Risk (Level I):**

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer shall be met.

⇒ **Medium Risk (Level II):**

Customers that are likely to pose a higher than average risk to the broker may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

- Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.

- Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious.

⇒ **High Risk (Level III):**

The dealers may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk

customers, especially those for whom the sources of funds are not clear. The examples of customers requiring higher due diligence may include

a) Non Resident Customers,
b) High Net worth individuals
c) Trusts, charities, NGOs and organizations receiving donations,
d) Companies having close family shareholding or beneficial ownership
e) Firms with 'sleeping partners'
f) Politically Exposed Persons (PEPs) of foreign origin
g) Non-face to face customers, and
h) Those with dubious reputation as per public information available, etc.

The persons requiring very high level of monitoring may be categorized as **Level IV**.

3. Customer Identification Procedure (CIP)

- Customer identification means identifying the person and verifying his/her identity by using reliable, independent source documents, data or information. The dealers need to obtain sufficient information necessary to establish, **to their satisfaction**, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of brokering relationship. Being satisfied means that the dealer is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance of the extant guidelines in place. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc). For customers that are natural persons, the dealers shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the dealers shall (i) verify the legal status of the legal person/entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person. Customer Identification

requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in Annexure I for the guidance of dealers.

- If the dealer decides to accept such accounts in terms of the Customer Acceptance Policy, the dealer shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are. An indicative list of the nature and type of documents/information that may be relied upon for customer identification is given in Annexure – II.

4. Monitoring of Transactions

- Continuous monitoring is an essential ingredient of effective KYC procedures and the extent of monitoring should be according to the risk sensitivity of the account. Dealers shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Transactions that involve large amount of cash inconsistent with the size of the balance maintained may indicate that the funds are being 'washed' through the account. High risk accounts shall be subjected to intensive monitoring.

- The Compliance Department shall ensure adherence to the KYC policies and procedures. Concurrent/Internal Auditors shall specifically check and verify the application of KYC procedures and comment on the lapses if any observed in this regard. The compliance in this regard shall be put up before the Meeting of the Board on quarterly intervals. All staff members shall be provided training on Anti Money Laundering. The focus of training shall be different for frontline staff, compliance staff and staff dealing with new customers.

5. Risk Management

- The broker's KYC policies and procedures covers management oversight, systems and controls, segregation of duties, training and other related matters. For ensuring effective implementation of the broker's KYC polices and procedures, the dealers shall explicitly allocate responsibilities within the branch. The Branch Dealer shall authorize the opening of all new accounts.

The dealers shall prepare risk profiles of all their existing and new customers and apply Anti Money Laundering measures keeping in view the risks involved in a transaction, account or brokering/business relationship.

- Training encompassing applicable money laundering laws and recent trends in money laundering activity as well as the broker's policies and procedures to combat money laundering shall be provided to all the staff members of the broker periodically in phases.

- The Accounts Department shall be empowered to prescribe threshold limits for a particular group of accounts and the dealers shall pay particular attention to the transactions which exceed these limits. The threshold limits shall be reviewed annually and changes, if any, conveyed to dealers for monitoring.

6. Customer Education

Implementation of KYC procedures requires dealers to demand certain information from the customers that may be of personal in nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Therefore, the front desk staff needs to handle such situations tactfully while dealing with customers and educate the customer of the objectives of the KYC programme. The dealers shall also be provided specific literature/pamphlets to educate customers in this regard.

7. New Technologies

The KYC procedures shall invariably be applied to new technologies to such other product which may be introduced by the broker in future that might favour anonymity, and take measures, if needed to prevent their use in money laundering schemes.

Dealers should ensure that appropriate KYC procedures are duly applied before issuing the clientcode to the customers. It is also desirable that if at any point of

time broker appoints/engages agents for marketing of products are also subjected to KYC measures.

While, the revised guidelines shall apply to all new customers/accounts, dealers shall apply these to the existing customers on the basis of materiality and risk. However, transactions in existing accounts shall be continuously monitored and any unusual pattern in the operation of the account should trigger a review of the Customer Due Diligence (CDD) measures. It has however to be ensured that all the existing accounts of companies, firm, trusts, charitable, religious organizations and other institutions are subjected to minimum KYC standards which would establish the identity of the natural/legal person and those of the 'beneficial owners'.

8. Appointment of Principal Officer

To ensure compliance, monitoring and report compliance of Anti Money Laundering policy of the broker, Senior Executive heading the Compliance Department of the broker at Corporate Office shall act as Principal Officer. He/She shall be responsible to monitor and report transactions and share information on Anti Money Laundering as required under the law. The Principal Officer shall maintain close liaison with enforcement agencies, brokers and any other institutions that are involved in the fight against money laundering and combating financing of terrorism. The Principal Officer shall furnish a compliance certificate to the Board on quarterly basis certifying that Revised Anti Money laundering Policy is being strictly followed by all the dealers of the broker.

Annexure- I

Customer Identification Requirements – Indicative Guidelines

Particulars	Guidelines
Trust/Nominee or Fiduciary Accounts	There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. The dealers should determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, dealers shall insist on receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, dealers should take reasonable precautions to verify the identity of the trustees and the settlers of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries should be identified when they are defined. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.
Accounts of companies and firms	Dealers need to be vigilant against business entities being used by individuals as a 'front' for maintaining accounts with brokers. Dealers should examine the control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management. These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders. But at least promoters, directors and its executives need to be identified adequately.
Client accounts opened by professional intermediaries	When the dealer has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Dealers may hold 'pooled' accounts managed by professional intermediaries on behalf of Entities like mutual funds, pension funds or other types of funds. Dealers should also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the Intermediaries are not co-mingled at the branch and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such accounts are co-mingled at the branch, the branch should still look through to the beneficial owners. Where the broker rely on the 'customer due diligence' (CDD) done by an intermediary, it shall satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements.
Accounts of Politically Exposed Persons(PEPs) resident outside India	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. Dealers should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Dealers should verify the identify of the person and seek information about the sources of funds before accepting the PEP as a customer. The dealers should seek prior approval of their concerned Heads for opening an account in the name of PEP.
Accounts of non-face-to-face customers	With the introduction of telephone and electronic brokering, increasingly accounts are being opened by brokers for customers without the need for the customer to visit the broker branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, there must be specific and adequate procedures to mitigate the higher risk involved. Certification of all the documents presented shall be insisted upon and, if necessary, additional documents may be called for. In such cases, dealers may also require the first payment to be effected through the customer's account if any with another broker which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and the dealers might have to rely on third party certification/introduction. In such cases, it must be ensured that the third party is a

	regulated and supervised entity and has adequate KYC systems in place.

Annexure-II

Customer Identification Procedure

Features to be verified and documents that may be obtained from Customers

Features	Documents
Accounts of individuals	• Legal name and any other names used • Correct permanent address (i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving licence (v) Identity card (subject to the satisfaction of the branch) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of branch (vii) Telephone bill (viii) Broker account statement (ix) Letter from any recognized public authority (x) Telephone bill (xi) Electricity Bill (xii) Ration Card (xiv) Letter from the employer, (subject to the satisfaction of the branch) (xv) Any other document which provides customer information to the satisfaction of the broker will suffice.
Accounts of companies	• Name of the company • Principal place of business • Mailing address of the company • Telephone/Fax Number (i) Certificate of incorporation and Memorandum & Articles of Association (ii)Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf

	(iv) Copy of PAN allotment letter (v) Copy of the telephone bill
Accounts of partnership firms	• Legal name • Address • Names of all partners and their addresses • Telephone numbers of the firm and partners (i) Registration certificate, if registered (ii) Partnership deed (iii)Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners
Accounts of trusts & foundations	• Names of trustees, settlers, beneficiaries and signatories • Names and addresses of the founder, the managers/directors and the beneficiaries • Telephone/fax numbers (i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses (iv) Resolution of the managing body of the foundation/association (v) Telephone bill

POLICIES AND PROCEDURE FOR PREVENTION OF MONEY LAUNDERING
(As per the requirements of the PMLA Act 2002)

1. **Firm Policy**
   It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.
2. **Principal Officer Designation and Duties**
   The firm has a Principal Officer for its Anti-Money Laundering Program, who takes full responsibility for the firm's AML program and is qualified by experience, knowledge and training . The duties of the Principal Officer will include monitoring the firm's compliance with AML obligations and overseeing communication and training for employees. The Principal Officer will also ensure that proper AML records are kept. When warranted, the Principal Officer will ensure filing of necessary reports with the Financial Intelligence Unit (FIU – IND)
3. **Customer Identification and Verification**
   At the time of opening an account or executing any transaction with it, the firm will verify and maintain the record of identity and current address or addresses including permanent address or addresses of the client, the nature of business of the client and his financial status as under

Constitution of Client	**Proof of Identity**	**Proof of Address**	**Others**
Individual	1. PAN Card	2. Copy of Bank Statement, etc	3. N.A.
Company	4. PAN Card 5. Certificate of incorporation 6. Memorandum and Articles of Association 7. Resolution of Board of Directors	8. As above	9. Proof of Identity of the Directors/ Others authorized to trade on behalf of the firm
Partnership Firm	10. PAN Card 11. Registration Certificate 12. Partnership deed	13. As above	14. Proof of Identity of the Partners/Others authorized to trade on behalf of the firm
Trust	15. PAN Card 16. Registration certificate	18. As above	19. Proof of Identity of the

	17. Trust deed		Trustees/others authorized to trade on behalf of the trust
AOP/BOI	20. PAN Card 21. Resolution of the managing body 22. Documents to collectively establish the legal existence of such an AOP/BOI	23. As above	24. Proof of Identity of the Persons authorized to trade on behalf of the AOP/BOI

25. If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our firm will not open the new account.
26. All PAN Cards received will verified form the Income Tax/ NSDL website before the account is opened.
27. The firm will maintain records of all identification information for ten years after the account has been closed.

4. Maintenance of records

The Principal Officer will be responsible for the maintenance for following records:

- all cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- all series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;
- all cash transaction 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;
- all suspicious transactions whether or not made in cash. Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith –
  - gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
  - appears to be made in circumstances of unusual or unjustified complexity; or
  - appears to have no economic rationale or bonafide purpose; or
  - gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism

The records shall contain the following information:

- the nature of the transactions;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

The records will be updated on daily basis, and in any case not later than 5 working days

5. Monitoring Accounts For Suspicious Activity

The firm will monitor through the automated means of Back Office Software for unusual size, volume, pattern or type of transaction. For non automated monitoring, the following kinds of activities are to be mentioned as Red Flags and reported to the Principal Officer.

- The customer exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents.
- The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer's stated business or investment strategy.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil or regulatory violations.
- The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.
- The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the Rs. 10,00,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer insists for multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the firm's normal documentation requirements.

- The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as Z group and T group stocks, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy or the customer's activity.)
- The customer's account shows an unexplained high level of account activity.
- The customer maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose.
- The customer's account has inflows of funds or other assets well beyond the known income or resources of the customer.

When a member of the firm detects any red flag he or she will escalate the same to the Principal Officer for further investigation.

Broad categories of reason for suspicion and examples of suspicious transactions for an intermediary are indicated as under:

i. Identity of Client
   - False identification documents
   - Identification documents which could not be verified within reasonable time
   - Non-face to face client
   - Doubt over the real beneficiary of the account.
   - Accounts opened with names very close to other established business entities

ii. Suspicious Background
   - Suspicious background or links with known criminals

iii. Multiple Accounts
   - Large number of accounts having a common account holder, introducer or authorized signatory with no rationale.
   - Unexplained transfers between multiple accounts with no rationale

iv. Activity in Accounts
   - 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

v. Nature of Transactions
   - Unusual or unjustified complexity
   - No economic rationale or bonafide purpose
   - Source of funds are doubtful
   - Appears to be case of insider trading
   - Investment proceeds transferred to a third party
   - Transactions reflect likely market manipulations
   - Suspicious off market transactions

vi. Value of Transactions
   - Value just under the reporting threshold amount in an apparent attempt to avoid reporting

- Large sums being transferred from overseas for making payments
- 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

6. Reporting to FIU IND

For Cash Transaction Reporting

- All dealing in Cash that requiring reporting to the FIU IND will be done in the CTR format and in the matter and at intervals as prescribed by the FIU IND

For Suspicious Transactions Reporting

We will make a note of Suspicion Transaction that have not been explained to the satisfaction of the Principal Officer and thereafter report the same to the FIU IND and the required deadlines. This will typically be in cases where we know, suspect, or have reason to suspect:

- the transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade any the transaction reporting requirement,
- the transaction is designed, whether through structuring or otherwise, to evade the any requirements of PMLA Act and Rules framed thereof
- the transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or
- the transaction involves the use of the firm to facilitate criminal activity.

We will not base our decision on whether to file a STR solely on whether the transaction falls above a set threshold. We will file a STR and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities.

All STRs will be reported quarterly to the Board of Directors, with a clear reminder of the need to maintain the confidentiality of the STRs

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the PMLA Act and Rules thereof.

7. AML Record Keeping

i. STR Maintenance and Confidentiality

We will hold STRs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency or securities regulator about a STR. We will refuse any requests for STR information and immediately tell FIU IND of any such request we receive. We will segregate STR filings and copies of supporting documentation from other firm books and records to avoid disclosing STR filings. Our Principal Officer will handle all requests or other requests for STRs.

ii. Responsibility for AML Records and SAR Filing

Principal Officer will be responsible to ensure that AML records are maintained properly and that STRs are filed as required.

iii. Records Required

As part of our AML program, our firm will create and maintain STRs and CTRs and relevant documentation on customer identity and verification. We will maintain STRs and their accompanying documentation for at least ten years.

8. **Training Programs**

We will develop ongoing employee training under the leadership of the Principal Officer. Our training will occur on at least an annual basis. It will be based on our firm's size, its customer base, and its resources.

Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employee's duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PMLA Act.

We will develop training in our firm, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

9. **Programe to Test AML Program**

   i. **Staffing:** The testing of our AML program will be performed by the Statutory Auditors of the company

   ii. **Evaluation and Reporting:** After we have completed the testing, the Auditor staff will report its findings to the Board of Directors. We will address each of the resulting recommendations.

10. **Monitoring Employee Conduct and Accounts**

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. We will also review the AML performance of supervisors, as part of their annual performance review. The Principal Officer's accounts will be reviewed by the Board of Directors

11. **Confidential Reporting of AML Non-Compliance**

Employees will report any violations of the firm's AML compliance program to the Principal Officer, unless the violations implicate the Principal/Compliance Officer, in which case the employee shall report to the Chairman of the Board. Such report will be confidential, and the employee will suffer no retaliation for making them.

12. **Board of Directors Approval**

We have approved this AML program as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements of the PMLA and the implementing regulations under it.

KMS STOCK BROKING COMPANY PVT LTD

ANAND KANAKIA
PRINCIPAL OFFIVER
Director/Authorised Signatory

ADDITIONAL LITERATURE FOR AML REQUIRMENTS

As per the requirements of SEBI, implementation of Anti Money Laundering (AML)/ Combating Financing of Terrorism requires trading members as intermediaries to demand certain information from investors which may be of personal nature or has hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions with regard to the motive and purpose of collecting such information. To, sensitize about these requirements as the ones emanating from AML and CFT framework, General FAQs as published by The Financial Action Task Force (FATF), an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing is reproduced herewith. Kindly feel free to visit the websites of http://www.fatf-gafi.org/ and http://fiuindia.gov.in for more information on the subject

FAQ

What is Money Laundering?

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

Illegal arms sales, smuggling, and the activities of organised crime, including for example drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery and computer fraud schemes can also produce large profits and create the incentive to “legitimise” the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

In response to mounting concern over money laundering, the Financial Action Task Force on money laundering (FATF) was established by the G-7 Summit in Paris in 1989 to develop a co-ordinated international response. One of the first tasks of the FATF was to develop Recommendations, 40 in all, which set out the measures national governments should take to implement effective anti-money laundering programmes.

How much money is laundered per year?

By its very nature, money laundering is an illegal activity carried out by criminals which occurs outside of the normal range of economic and financial statistics. Along with some other aspects of underground economic activity, rough estimates have been put forward to give some sense of the scale of the problem.

The International Monetary Fund, for example, has stated in 1996 that the aggregate size of money laundering in the world could be somewhere between two and five percent of the world’s gross domestic product.

Using 1996 statistics, these percentages would indicate that money laundering ranged between US Dollar (USD) 590 billion and USD 1.5 trillion. The lower figure is roughly equivalent to the value of the total output of an economy the size of Spain.
However it must be said that overall it is absolutely impossible to produce a reliable estimate of the amount of money laundered and therefore the FATF does not publish any figures in this regard.

How is money laundered?

In the initial - or placement - stage of money laundering, the launderer introduces his illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location.
After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sales of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not co-operate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance.
Having successfully processed his criminal profits through the first two phases the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy. The launderer might choose to invest the funds into real estate, luxury assets, or business ventures.

Where does money laundering occur?

As money laundering is a consequence of almost all profit generating crime, it can occur practically anywhere in the world. Generally, money launderers tend to seek out countries or sectors in which there is a low risk of detection due to weak or ineffective anti-money laundering programmes. Because the objective of money laundering is to get the illegal funds back to the individual who generated them, launderers usually prefer to move funds through stable financial systems.
Money laundering activity may also be concentrated geographically according to the stage the laundered funds have reached. At the placement stage, for example, the funds are usually processed relatively close to the under-lying activity; often, but not in every case, in the country where the funds originate.
With the layering phase, the launderer might choose an offshore financial centre, a large regional business centre, or a world banking centre – any location that provides an adequate financial or business infrastructure. At this stage, the laundered funds may also only transit bank accounts at various locations where this can be done without leaving traces of their source or ultimate destination.
Finally, at the integration phase, launderers might choose to invest laundered funds in still other locations if they were generated in unstable economies or locations offering limited investment opportunities.

S

How does money laundering affect business?

The integrity of the banking and financial services marketplace depends heavily on the perception that it functions within a framework of high legal, professional and ethical standards. A reputation for integrity is the one of the most valuable assets of a financial institution.

If funds from criminal activity can be easily processed through a particular institution – either because its employees or directors have been bribed or because the institution turns a blind eye to the criminal nature of such funds – the institution could be drawn into active complicity with criminals and become part of the criminal network itself. Evidence of such complicity will have a damaging effect on the attitudes of other financial intermediaries and of regulatory authorities, as well as ordinary customers.

As for the potential negative macroeconomic consequences of unchecked money laundering, one can cite inexplicable changes in money demand, prudential risks to bank soundness, contamination effects on legal financial transactions, and increased volatility of international capital flows and exchange rates due to unanticipated cross-border asset transfers. Also, as it rewards corruption and crime, successful money laudering damages the integrity of the entire society and undermines democracy and the rule of the law.

What influence does money laundering have on economic development?

Launderers are continuously looking for new routes for laundering their funds. Economies with growing or developing financial centres, but inadequate controls are particularly vulnerable as established financial centre countries implement comprehensive anti-money laundering regimes.

Differences between national anti-money laundering systems will be exploited by launderers, who tend to move their networks to countries and financial systems with weak or ineffective countermeasures.

Some might argue that developing economies cannot afford to be too selective about the sources of capital they attract. But postponing action is dangerous. The more it is deferred, the more entrenched organised crime can become.

As with the damaged integrity of an individual financial institution, there is a damping effect on foreign direct investment when a country's commercial and financial sectors are perceived to be subject to the control and influence of organised crime. Fighting money laundering and terrorist financing is therefore a part of creating a business friendly environment which is a precondition for lasting economic development.

What is the connection with society at large?

The possible social and political costs of money laundering, if left unchecked or dealt with ineffectively, are serious. Organised crime can infiltrate financial institutions, acquire control of large sectors of the economy through investment, or offer bribes to public officials and indeed governments.

The economic and political influence of criminal organisations can weaken the social fabric, collective ethical standards, and ultimately the democratic institutions of society.

In countries transitioning to democratic systems, this criminal influence can undermine the transition. Most fundamentally, money laundering is inextricably linked to the underlying criminal activity that generated it. Laundering enables criminal activity to continue.

How does fighting money laundering help fight crime?

Money laundering is a threat to the good functioning of a financial system; however, it can also be the Achilles heel of criminal activity.

In law enforcement investigations into organised criminal activity, it is often the connections made through financial transaction records that allow hidden assets to be located and that establish the identity of the criminals and the criminal organisation responsible.

When criminal funds are derived from robbery, extortion, embezzlement or fraud, a money laundering investigation is frequently the only way to locate the stolen funds and restore them to the victims.

Most importantly, however, targeting the money laundering aspect of criminal activity and depriving the criminal of his ill-gotten gains means hitting him where he is vulnerable. Without a usable profit, the criminal activity will not continue.

What should individual governments be doing about it?

A great deal can be done to fight money laundering, and, indeed, many governments have already established comprehensive anti-money laundering regimes. These regimes aim to increase awareness of the phenomenon – both within the government and the private business sector – and then to provide the necessary legal or regulatory tools to the authorities charged with combating the problem.

Some of these tools include making the act of money laundering a crime; giving investigative agencies the authority to trace, seize and ultimately confiscate criminally derived assets; and building the necessary framework for permitting the agencies involved to exchange information among themselves and with counterparts in other countries.

It is critically important that governments include all relevant voices in developing a national anti-money laundering programme. They should, for example, bring law enforcement and financial regulatory authorities together with the private sector to enable financial institutions to play a role in dealing with the problem. This means, among other things, involving the relevant authorities in establishing financial transaction reporting systems, customer identification, record keeping standards and a means for verifying compliance.

Should governments with measures in place still be concerned?

Money launderers have shown themselves through time to be extremely imaginative in creating new schemes to circumvent a particular government's countermeasures. A national system must be flexible enough to be able to detect and respond to new money laundering schemes.

Anti-money laundering measures often force launderers to move to parts of the economy with weak or ineffective measures to deal with the problem. Again, a national system must be flexible enough to be able to extend countermeasures to new areas of its own economy. Finally, national governments need to work with other jurisdictions to ensure

that launderers are not able to continue to operate merely by moving to another location in which money laundering is tolerated.

S

What about multilateral initiatives?

Large-scale money laundering schemes invariably contain cross-border elements. Since money laundering is an international problem, international co-operation is a critical necessity in the fight against it. A number of initiatives have been established for dealing with the problem at the international level.

International organisations, such as the United Nations or the Bank for International Settlements, took some initial steps at the end of the 1980s to address the problem. Following the creation of the FATF in 1989, regional groupings – the European Union, Council of Europe, Organisation of American States, to name just a few – established anti-money laundering standards for their member countries. The Caribbean, Asia, Europe and southern Africa have created regional anti-money laundering task force-like organisations, and similar groupings are planned for western Africa and Latin America in the coming years.

S

Client Sign Place MUMBAI Date