

POLICIES AND PROCEDURE FOR
PREVENTION OF
MONEY LAUNDERING

For & Exclusive use of KGSBPL

Reviewed on 14.07.15

Revised on 21.04.14

Khajanchi & Gandhi Stock Broking Pvt. Ltd.

Background

The prevention of Money Laundering Act , 2002 (PMLA) has been brought in force with effect from 1st July 2005 and it provides for Anti-Money Laundering and Anti-terrorist Financing measures to be taken in India and the rules framed there under provides guidance on the practical implementation of the provisions laid down in the Act. The Director appointed by Financial Intelligence Unit- INDIA (FIU-INDIA) has been conferred with exclusive and concurrent powers under relevant sections of the Act to implement its provisions. The Act imposes an obligation on banking companies, financial institutions and intermediaries associated with the securities market and registered with Securities and Exchange Board of India (SEBI) under Section 12 of SEBI Act, 1992. The stock brokers fall under the category of intermediaries under Section 12 of the SEBI Act, 1992 and hence the provisions of PMLA are also applicable to all the stock brokers. Establishment of Anti-Money Laundering programs by Market Intermediaries are one of the recommendations of the Financial Action Task Force (FATF).

SEBI has issued necessary directives from time to time vide its circulars covering issues related to Know Your client (KYC) norms , Anti-Money Laundering (AML), Client Due Diligence (CDD) and Combatting Financing of Terrorism (CFT). This policy document is based on SEBI's master circular on PMLA bearing reference No. CIR/ISD/AML/3/2010 dated 31-Dec-2010 which consolidates requirements/obligations to be fulfilled by all the registered intermediaries.

This policy will be subject to change in order to incorporate further directives that SEBI may give vide its circulars on PMLA, from time to time.

What is Money Laundering?

Money Laundering is the processing of criminal proceeds to disguise their illegal origin. It is a process by which persons with criminal intent or persons involved in criminal activities attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of illegal funds.

Financial Intelligence Unit (FIU)- India

Financial Intelligence Unit – India (FIU-IND) was set by the Government of India on 18th November 2004 as the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspicious financial transactions. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

Anti-Money Laundering Program

The objective of having an AML program is to have in place adequate policies and procedures that help to prevent money-laundering activities. Such procedures would include the following:

Appointment of Principal Officer & Designated Director:

The management of the company has designated Mr. Darshan Shah as the Principal Officer & Designated Director for its Anti-Money Laundering Program, with full responsibility for the company's AML program.

Responsibility of Principal Officer & Designated Director:

The Principal Officer shall ensure that the PMLA guidelines and PMLA Policy is effectively implemented by the company.

- The monitoring of transactions is done on a regular basis.
- Reporting of suspicious transactions to the prescribed authorities in the specified time limit.
- To maintain the record of all the transactions, its nature and value
- To update the management regarding any changes / additions and modifications in the PMLA provisions.
- To co-operate and submit the required information to the regulating agencies within the required time.

The company has provided the FIU with contact information for the Principal Officer, including name, title, mailing address, e-mail address, telephone number and facsimile number. The company will promptly notify FIU of any change to this information.

Client Due Diligence Process:

The Overall Client Due Diligence Process comprises of the following three specific parameters:

- A) Client acceptance policy
- B) Client Identification Process
- C) Monitoring of transactions and Reporting

A. Client acceptance policy:

It is essential to make reasonable efforts to determine the true identity of the clients and the company shall put in place effective procedures to obtain requisite details for proper identification of new clients.

- All KYC documentation and procedures prescribed by the Exchanges and SEBI shall be followed at the time of account opening.
- To clearly establish the identity of the client, verification of the addresses and other details. To verify the genuineness of the PAN provided by the client by comparing with the original PAN and checking with Income-Tax website. To verify the copies with the original documents.
- The In-person verification of the client has to be done by the employees of the company.
- To verify whether the client at any point of time has been banned from trading in the stock market by SEBI or any other regulatory authority.
- To verify whether the client has any criminal background and whether he has been at any point of time been associated with any civil or criminal proceedings anywhere.
- To verify whether the client is a politically exposed person or is a relative of a politically exposed person.
- To ensure that no account is opened in a fictitious/benami name and also where the concerned official is unable to apply appropriate client due diligence measures/KYC policies. Incomplete documentation and incomplete application should be rejected.
- To obtain sufficient information in order to identify persons who beneficially own or control the trading account.

The company shall categorize its clients into low, medium and high risk as per its categorization process and thereafter collect documents and other information from the clients based on the perceived risk in order to achieve the PMLA objective.

B. Client Identification and Verification

At the time of opening an account or executing any transaction with it, the company 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	<ul style="list-style-type: none">• PAN Card	<ul style="list-style-type: none">• Copy of Bank Statement, etc	<ul style="list-style-type: none">• N.A.
Company	<ul style="list-style-type: none">• PAN Card• Certificate of incorporation• Memorandum and Articles of Association• Resolution of Board of Directors	<ul style="list-style-type: none">• As above	<ul style="list-style-type: none">• Proof of Identity of the Directors/Others authorized to trade on behalf of the Company
Partnership Company	<ul style="list-style-type: none">• PAN Card• Registration certificate• Partnership deed	<ul style="list-style-type: none">• As above	<ul style="list-style-type: none">• Proof of Identity of the Partners/Others authorized to trade on behalf of the company
Trust	<ul style="list-style-type: none">• PAN Card• Registration certificate• Trust deed	<ul style="list-style-type: none">• As above	<ul style="list-style-type: none">• Proof of Identity of the Trustees/ others authorized to trade on behalf of the trust
AOP/ BOI	<ul style="list-style-type: none">• PAN Card• Resolution of the managing body• Documents to collectively establish the legal existence of such an AOP/ BOI	<ul style="list-style-type: none">• As above	<ul style="list-style-type: none">• Proof of Identity of the Persons authorized to trade on behalf of the AOP/ BOI

1. 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 company will not open the new account.
2. All PAN Cards received will be verified from the Income Tax/ NSDL website before the account is opened
3. The documents provided by the clients will be reviewed on a periodic basis, mostly yearly and will be updated as per the latest requirements and guidelines of the regulatory bodies.

Risk Categorization

The company shall categorize its clients into high medium, and low risk as per its categorization process and thereafter collect documents and other information from the clients based on the perceived risk in order to achieve the PMLA objective.

Clients should broadly be classified in the following categories:

RISK	PARTICULARS
High Risk	Clients which are likely to pose a high risk to the company, may be categorized as high risk. -Clients who have defaulted in the past, -Clients who have a suspicious background -HNIs whose identity and source of wealth are difficult to identify -Politically exposed persons , -Clients of Special Category, -Dormant Account
Medium Risk	Clients which are likely to pose a medium risk to the company, may be categorized as medium risk. They can be the following: -Where the client profile of the person opening the account is doubtful or dubious. -Where the trading and settlement pattern of the client is suspicious -Intraday clients or speculative client.
Low Risk	Clients who pose low or nil risk. -They are corporate/HNIs/ Professionals who have a respectable social and financial standing. -Clients who fulfill obligations on time.

Initial Risk categorization of all the clients would be done by the company, at the time of opening of the Client accounts, depending on the financials details/ net-worth declarations and KYC declaration so of the clients given by the clients at time of account opening and regular updates received from the clients and shall be reviewed on an ongoing basis.

Risk Assessment

Risk assessment has been done to identify, assess, and take effective measures to mitigate money laundering and terrorist financing risk with respect to clients, countries or geographical areas, nature and volume of transactions, payment method used by clients, etc. It also include any country specific information circulated by Government of India, SEBI etc. from time to time and updated list of individuals and entities who are subjected to sanction measures as required under United Nation's Security Council Resolutions. This assessment will be properly documented, regularly updated and made available to competent authorities and self-regulating bodies as and when required.

Client of Special Category

Due care shall be taken while accepting clients of Special category.

Clients of Special Category include but shall not be limited to the following

- ❖ Non Residents Clients
- ❖ High Net Worth Clients
- ❖ Trust, Charities, Non- Government Organizations (NGOs) and Organizations receiving donations.
- ❖ Companies having close family shareholdings or beneficial ownership
- ❖ Politically exposed persons (PEP) of foreign origin
- ❖ Companies offering foreign exchange offerings
- ❖ Clients in high risk countries
- ❖ Non face to face clients
- ❖ Clients with dubious reputation as per public information available

TREATMENT OF ACCOUNTS OF CLIENTS OF SPECIAL CATEGORY

1. NRI: - While opening NRI account utmost care should be exercised. Collect the following documents

- ❖ PAN Card Copy
- ❖ Pass Port Copy with date of arrival in case personal visit
- ❖ Indian & foreign Address Proof
- ❖ Cancelled cheque copy of NRE A/c, along with PIS permission issued from RBI & Bank statement copy
- ❖ Client master copy for demat account
- ❖ FEMA declaration

2. High Net worth Clients:-High Net worth clients could be classified as such if at the account opening stage or during the course of the relationship, it is realized that the client's investments or the appropriate for investment is high.

3. Trust, Charity and NGOs: -Public as well as private, registered as well as unregistered trust will have to be classified in the special category.

4. Politically Exposed Person: - In case of PEPs, the account should be opened only after consent of the senior management and principal officer & all the required documents are collected and client should be marked as PEP in records. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.

Monitoring Accounts for Suspicious Activity

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

The customer exhibits unusual concern about the company's compliance with government reporting requirements and the company'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.

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 company's normal documentation requirements.

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.

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

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
- Suspicious Background
- Suspicious background or links with known criminals

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 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;
- 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
In terms of rules made under the PMLA Act, KGSBPL shall maintain and preserve a record of:

(a) All suspicious transactions whether or not made in cash **for a period of Five years**;

(b) 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, account files, business correspondence and all other details as per PMLA guide line **for a period of Five years after the business relationship between client and intermediary has ended or the account has been closed whichever is later** .

(c) Suspicious records along with the records of the identity of clients shall be maintained and preserved **for a period of Five years** or as may be in force from time to time from the date of cessation of the transaction between the Client and intermediaries

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 at intervals as prescribed by the FIU IND.

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 company 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.

DUE DATE FOR REPORTING:

Cash Transaction Report: **15th Day** of the Succeeding month

Suspicious Transaction Report: **7th Day** of the succeeding month

AML Record Keeping

a. 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 company books and records to avoid disclosing STR filings. Our Principal Officer will handle all requests or other requests for STRs.

b. 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

c. Records Required

As part of our AML program, our company 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 **Five years** or as may be in force from time to time from the date of cessation of the transaction between the Client and intermediaries

High standards in hiring policies and training with respect to anti money laundering

The company has adequate screening procedures in place to ensure high standards when hiring employees. The company will identify properly the key position within the organization structure having regard to the risk of money laundering and terrorist financing and size of their business. The senior management level has been entrusted with the responsibility of complying with the provisions of the ACT and reporting of the suspicious transactions, if any. The employees of the company has been briefed up and trained with the provisions and intentions of the Act putting stress to anti money laundering and anti- terrorist financing.

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 company's size, customer base, and 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 employees' duties; what to do once the risk is identified; what employees' roles are in the company's compliance efforts and how to perform them; the company'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 company, or contract for it. Delivery of the training may include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos.

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

Confidential Reporting of AML Non-Compliance

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

Investors Education:

Implementation of AML/CFT measures require member 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 by the client with regard to the motive and purpose of collecting such information.

There is, therefore, a need for intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. Intermediaries shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

Policy Review and Updation

The policy will be reviewed and updated on a yearly basis by the management so as to update any policy level changes of the company and also, revised periodically to make it in line with the latest Rules, Regulations, Circulars & Guidelines of the SEBI, Exchanges and Depositories.

Approval from the Board

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

The board of director has accorded their consent in implementing this policy as on 14.07.15