

PMLA POLICY

Bigmans Consultant & Marketing Pvt. Ltd. (www.bigmansadvisory.com)

Registration Number: - INA000019123

Date of Registration:- 11th June 2024

POLICY FRAMEWORK FOR IMPLEMENTATION OF THE PROVISIONS OF PREVENTION AND MONEY LAUNDERING ACT (PMLA) 2002

Introduction

The Prevention of Money Laundering Act, 2002 (**PMLA**) came in force with effect from 1st July 2005. As per the provisions of the PMLA, each market intermediary (**Reporting Entity**) (which includes a stockbroker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depository participant, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with the securities market and registered under Section 12 of the Securities and Exchange Board of India Act, 1992 (**SEBI Act**) shall have to adhere to client account opening procedures and maintain records of such “transactions” as prescribed by the PMLA and Rules notified there under.

Obligations of a “Reporting Entity” includes:-

- a. to maintain a record of all transactions covered as per the nature and value of which may be prescribed, in such manner as to enable it to reconstruct individual transactions
- b. furnish to the Director (FIU) within such time as may be prescribed information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed
- c. verify the identity of its clients in such manner and subject to such conditions as may be prescribed
- d. identify the beneficial owner, if any, of such of its clients, as may be prescribed
- e. maintain record of documents evidencing identity of its clients and beneficial owners, account files and business correspondence relating to its clients and information related to transactions for specified period.

For the purpose of PMLA, transactions include:

- 1. all cash transactions of the value of more than Rs.10 Lakhs or its equivalent in foreign currency.
- 2. all series of cash transactions integrally connected to each other, which have been valued below Rs.10 Lakhs or its equivalent in foreign currency, such series of transactions within one calendar month.

3. all suspicious transactions (remotely / integrally connected or related), whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account maintained by the registered intermediary.

For the purpose “**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 proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or
- b. appears to be made in circumstances of unusual or unjustified complexity; or
- c. appears to have no economic rationale or confide purpose; or
- d. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

The Anti-Money Laundering Guidelines provides a general background on the subjects of money laundering and terrorist financing in India and provides guidance on the practical implications of the PMLA. The PMLA Guidelines sets out the steps that a registered intermediary and any of its representatives, need to implement to identify and discourage any “Money Laundering” (ML) or “Terrorist Financing” activities.

SEBI has issued various directives vide circulars, from time to time, covering issues related to Know Your Client (**KYC**) norms, Anti- Money Laundering (**AML**), Client Due Diligence (**CDD**) and Combating Financing of Terrorism (**CFT**). The directives lay down the minimum requirements and it is emphasized that the intermediaries may, according to their requirements, specify additional disclosures to be made by clients to address concerns of money laundering and suspicious transactions undertaken by clients.

While it is recognized that a “one-size-fits-all” approach may not be appropriate for the securities industry in India, each registered intermediary is required to implement suggested measures and procedures considering the specific nature of its business, organizational structure, type of clients and transactions, etc. to ensure that they are effectively applied.

Global measures taken to combat drug trafficking, terrorism and other organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. To be in compliance with these obligations, the senior management of a registered intermediary shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements.

The obligations of an intermediary under Prevention of Money Laundering Act,

2002 (PLMA) includes:-

- a. issuance and adoption of written policy statement, on a group basis (wherever applicable), for dealing with the risk of MF and TF within the framework of current statutory and regulatory requirements,
- b. ensuring that these directives and contents of policy is understood by all staff members,
- c. regular review of policy and procedures of prevention of ML & TF and to ensure that such reviews are conducted by the person other than the one framing the policy,
- d. adoption of client acceptance policies and procedures which are sensitive to the risk of MF & TF,
- e. undertaking client due diligence measures to an extent that is sensitive to the risk of ML & TF
- f. compliance with relevant statutory and regulatory requirements
- g. have system in place for identification, monitoring and reporting of suspected ML and TF transactions to concerned authorities
- h. co-operation with relevant law enforcement authorities and timely disclosure of information
- i. defining the role of internal auditors to ensure compliance of policies, procedures and control to prevent money laundering.

Accordingly, we have drafted this written policy framework (hereinafter called as "PMLA Policy") for **Bigmans Consultant & Marketing Pvt. Ltd. Trade name Bigmans Investment Adviser** for policy which aims to have a system in place to identify, monitor and reporting the suspected money laundering or terrorist financing transactions to law enforcing authorities within the framework of current statutory and regulatory requirements. All concerned are hereby advised to ensure that every possible measures are taken for the effective implementation of this Policy and that the measures taken are adequate, appropriate and abide by the spirit and requirements as enshrined in the PMLA.

Detailed PMLA Policy Framework

1. Principal Officer:

To ensure effective discharge of our legal obligations to report suspicious transactions to the authorities, we hereby appoint the "Principal Officer" who would act as a central reference point for the identification and assessment of potentially suspicious transactions and in facilitating onward reporting of suspicious transactions to FIU. Complete Details of Principle are as given below:-

Name: Dr. Suman Kumar

Designation: Compliance Officer

Contact no: +91-7992372875

Email: info@bigmansadvisory.com

Rights and Obligations of Principle Officer:

a. The principal office shall have all time access to customer identification data and other CDD information.

b. The principal officer shall have complete independence and authority to access .

Responsibilities:

The Principal Officer shall ensure that:

a. the approved PMLA Policy framework is implemented effectively.

b. systems generated data based on set parameters is regularly and promptly downloaded to analyze, identify and report transactions of suspicious nature to FIU-IND directly

c. group responds promptly to any request for information, including KYC related information maintained by us, made by the regulators, FIU-IND and other statutory authorities.

d. group`s staff members and associates are trained to address issues related to the application of the PMLA.

e. the staff selection and training process complies with the PMLA Policy.

f. group and all concerned staff is regularly updated regarding any changes / additions / modifications in PMLA provisions.

2. Client Due Diligence Measures (CDD Measures)

The CDD measures comprise the following:

a. Obtain sufficient information in order to identify persons who beneficially own or control the account party shall be identified using client identification and verification procedures.

b. Verify the client's identity using reliable, independent source documents, data or information;

c. Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted;

d. Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c);

e. Understand the ownership and control structure of the client;

f. Conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds; and

g. All documents, data or information of all clients and beneficial owners collected under the CDD process shall be periodically updated. The beneficial owner for this purpose mean, the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. Suggestive measures for identification of beneficial ownership is as given below:-

i.) 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, identification of beneficial owners of the client may be done by applying following measures namely; ascertain 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:

▮ more than 25% of shares or capital or profits of the juridical person, where the juridical person is a company;

▮ more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or

▮ 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.

In cases where there exists doubt 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.

Where no natural person is identified under clauses mentioned above, the identity of the relevant natural person who holds the position of senior managing official.

ii.) For client which is a trust:

Where the client is a trust, the beneficial ownership of the client shall be identifying by taking reasonable measures to verify 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.

iii.) Exemption in case of listed companies:

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.

Reliance on third party for carrying out due diligence

We may rely on a third party for the purpose of

- a. identification and verification of the identity of a client and
- b. where the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner.

provided such 3rd party is regulated, supervised or monitored for and have measures in place for CDD and KRA is one such example of the same.

However as a registered intermediary we shall be ultimately responsible for CDD and undertaking enhanced due diligence measures

4. Policy for acceptance of Clients

Our client acceptance policies and procedures aims to identify the types of clients that are likely to pose a higher than average risk of ML or TF so that we will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transactions.

In nutshell the following safeguards are to be followed while accepting the clients namely;

- a. No account is opened in a fictitious / benami name or on an anonymous basis.
- b. Each client shall be classified into low or medium or high risk categories depending upon the risk perception.

Such risk categorization may be arrived considering various factors of risk perception of the client having regard to:-

- clients' location (registered office address, correspondence addresses and other addresses if applicable),

- nature of business activity, trading turnover etc. and
- manner of making payment for transactions undertaken.

Clients of Special Category (CSC) (as defined later in this policy) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of Know Your Client (**KYC**) profile.

c. Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

d. We must obtain documentary evidence of each KYC information provided by the client and verify each such supporting document with originals prior to acceptance of a copy and same be stamped "Verified with the original" and each client must be met in person before registration.

The information collected by us should be enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by us in compliance with the Guidelines. A complete identification record of person doing the In-person verification and verification of documents must be kept in readily available manner.

e. We should not accept where we are unable to apply appropriate CDD measures / KYC policies. This shall be applicable in cases where it is not possible to ascertain the identity of the client, or the information provided by the client is suspected to be non-genuine, or there is perceived non co-operation of the client in providing full and complete information.

We shall not continue to do business with such a person and file a suspicious activity report. We shall also evaluate whether there is suspicious any trading in determining whether to freeze or close the account. We shall be cautious to ensure that we do not return securities or money that may be from suspicious trades.

Further, we shall consult the relevant authorities in determining what action we shall take when we suspects suspicious trading activity.

f. We shall ensure that in case of individual client only the client himself/ herself be allowed to transact on his/her own behalf. A person may be allowed to deal on behalf of his / her spouse, dependent children or dependent parents provided a written authorization is obtained from concerned family member.

In case of non-individual clients only the person(s) having appropriate written authorization are allowed to deal for and on behalf of the client.

In all the cases, we must obtain the identification documents of the person so authorized to deal on behalf of the client and adequate verification of person's authority to act on behalf of the client shall also be carried out.

The authorization letter should specify the manner in which the account shall be operated, transaction limits for the operation, additional authority (if any) required for transactions exceeding a specified quantity/value.

g. Before activating any service, we must ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets / accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at <http://www.un.org>.

h. The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

For the purpose of above and elsewhere used in this policy framework, Clients of Special Category (**CSC**) shall include:-

i.) Non resident clients

ii.) High net-worth clients unless known to Senior Management or introduced by a known source,

iii.) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations

iv.) Companies having close family shareholdings or beneficial ownership

v.) Politically Exposed Persons (**PEP**) 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.

vi.) Companies offering foreign exchange offerings

vii.) Clients in high risk countries where existence / effectiveness of money laundering controls is suspect, 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. While dealing with clients in high risk countries where the existence/effectiveness of money laundering control is suspect, intermediaries apart from being guided by the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), shall also independently access and consider other publicly available information.

viii.) Non face to face clients

ix.) Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and the intermediary shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

5. Risk-Based Approach to KYC

Client acceptance is a critical activity in AML compliance. Registering any client means providing such client with an entry point to local and international financial systems. Client acceptance, thus, becomes the first step in controlling money laundering and terrorist financing. Regulatory guidelines stipulate that a sound KYC program should determine the true identity and existence of the customer and the risk associated with the customer. It is therefore imperative that we capture information about their background, sources of funds, nature and type of business, domicile and financial products used by them and how these are delivered to them in order to properly understand their risk profile. It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. The basic principle enshrined in this approach is that the registered intermediaries shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that we shall obtain necessarily depend on the risk category of a particular client and for this purpose clients may be classified into following categories namely;-

Category – A : Medium Risk

Category – B : High Risk, should be classified as

.

Category “A” clients are those who mostly deals on intra-day basis or on speculative basis. These are the clients who maintain running services with the Company.

Category “B” clients are those who have defaulted in the past, have suspicious background or the clients identified as CSC.

Any business relationship with “High Risk Clients” including clients identified as CSC must not be commenced unless approved by Senior Management Officials.

As customer risk rating and KYC drives enhanced due diligence and ongoing monitoring it is critical that we conduct an ongoing comprehensive assessment to understand the risks associated with our business and customers and necessary modifications and improvements in associated Client acceptance and Due Diligence Policies and Procedures.

Risk Assessment

We have formulated a periodic risk assessment mechanism to identify money laundering and terrorist financing risk assess and take effective measures to mitigate them with respect to our clients, countries or geographical areas, nature and volume of transactions, payment methods used by our clients, etc. Our risk assessment process consider all the relevant factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied and assessment is documented and updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

6. Transaction based Monitoring and Identification of Suspicious Transactions

Ongoing monitoring is an essential element of effective KYC procedures. We can effectively control and reduce the risk only if we have an understanding of the normal and reasonable activity of the client so that they have the means of identifying transactions that fall outside the regular pattern of activity.

However, the extent of monitoring will depend on the risk sensitivity of the account.

Special attention is required to be given to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

For the purpose of monitoring of transaction under PMLA following should be taken care of:

- a. examine the background and the purpose of transactions which are complex or unusually large/ with patterns which appear to have no economic purpose
- b. transactions which exceed the limits specified for the relevant class of client accounts
- c. understanding of normal activity in client account to identify deviations and substantial increase in business without any apparent cause
- d. clients transferring large sums of money to/from overseas locations
- e. attempted transfer of proceeds to unrelated 3rd parties
- f. transactions of clients based in high risk jurisdictions
- g. Unusual transactions by CSCs and businesses undertaken by offshore banks / financial services, businesses reported to be in the nature of export- import of small items
- h. Random examination of a selection of transaction to comment on their nature

Broad category of triggers that will require the complete analysis of transaction may include:-

- a. Transactions involving Artificial Volume Creation / High Value Deals / Synchronized Trades

- b. client's disproportionate volume with respect to his last known financial details
- c. scrip concentration-concentrated position in particular scrips which have an unusual price or volumes
- d. high value off market transfer instructions
- e. high value transactions in a new/dormant account
- f. frequent small quantity transactions in an account
- g. transaction undertaken by client with respect to whom alerts raised by employees / media reports / Enforcement Agency etc.
- h. transactions undertaken by customers for whom there are adverse media reports about criminal activities/terrorist activities/terrorist financing activities
- i. transaction undertaken by customers who offered false/forged identification documents / address found to be wrong

Findings of transaction analysis must be recorded in writing, as the same along with records and related documents may required to be provided to auditors, SEBI, Stock Exchanges, FIUIND, other relevant authorities as and when asked for.

7. Reporting of Suspicious Transactions

The Principal Officer would act as a central reference point in playing an active role in the identification and assessment of potentially suspicious transactions and facilitating onward reporting of suspicious transactions.

Accordingly, any potential suspicious transaction shall immediately be notified to Principle Officer which may be a detailed report with specific reference to the clients, transactions and the nature / reason of suspicion and for this purpose transactions abandoned or aborted by clients on being asked to give some details or to provide documents are also to be reported.

We must ensure continuity in dealing with the reported client as normal until told otherwise and the client not be told of the report/suspicion i.e. group officials and employees shall be prohibited from "Tipping off" the fact that a STR or related information is being reported or provided to the FIU-IND.

The Principal Officer shall examine the transaction in details and if reaches to the conclusion that the notified transaction is "Suspicious" shall report the same to **Financial Intelligence Unit** (FIU) within 7 days from the date of arriving at such conclusion by filing the Suspicion Transaction Report (STR).

It is clarified that the STR must be filed irrespective of the amount of transaction and/or the threshold limit, if there are reasonable grounds to believe that the transactions involve proceeds of crime.

8. Record Keeping

We are required to maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

To enable this reconstruction, we need to retain the following information:-

- a. the nature of transaction
- b. the amount of transaction and the currency in which same was denominated
- c. the date on which the transaction was conducted and
- d. the parties to the transaction

We shall ensure maintaining proper record of transactions namely:-

- a. all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
- b. all series of cash transactions integrally connected to each other which have been valued below rupees ten 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 rupees ten 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

Records to be maintained in a way that all client and transaction records and information are available on a timely basis to the competent investigating authorities.

9. Retention of Records

Following Document Retention Terms should be observed:

- a. All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period of FIVE YEARS (5) from the date of cessation of the transaction.
- b. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

c. In situations where the records relate to on-going investigation 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.

d. All necessary records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, shall be maintained and preserved for a period of five years from the date of the transaction between the client and the intermediary.

Records may be maintained in both hard and / or soft copies.

10. Training of staff / Employees

All the staff members involved in front office dealings, back office, KYC & Compliances, Risk Management or any kind of client dealings need to be adequately trained in AML and CFT (Combating Financing of Terrorism) procedures. They should fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of our systems being misused by unscrupulous elements.

Accordingly, we have an ongoing employee-training programme (in-house as well as sending employees for attending of independent training workshops) so that the concerned staff are adequately trained in AML and CFT procedures.

Further, the Principle Officer is authorized to ensure that all the concerned staff is well versed with latest modifications in the PMLA policy framework and is adequately sensitized to the risks of ML & TF.

11. Employees Hiring

We have adequate screening procedures in place to ensure high standard when hiring employees. We have identified the key positions within the Company structure having regard to the risk of money laundering and terrorist financing.

The HR Department is instructed to verify the identity, cross check all the references, family background and should take adequate safeguards to establish the authenticity and genuineness of the persons before recruiting.

The department should obtain the following documents:

- 1 Photographs
- 2 Proof of address
- 3 Identity proof
- 4 Proof of Educational Qualification
- 5 Proof of Bank Account Details

12. Investor' Education

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which have 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 clients with regard to the motive and purpose of collecting such information. We, therefore need to sensitize prospective client that these requirements emanating from AML and CFT framework.

This may either be done by preparing specific literature or by educating the clients / sub-brokers / Authorised Person on the objectives of the Anti Money Laundering (AML) / Combating Financing of Terrorism (CFT) programme.

13. Review of PMLA/CFT Procedures

The policy shall be reviewed periodically so as to incorporate the latest change(s) in the Anti Money Laundering Act 2002 or change in any other act, bye-laws, rules, regulations of SEBI, CBI or in any statutory and regulatory government department related to or affect to this.

Further the review of this policy framework shall be undertaken by the person other than the one who has framed this policy.

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

Section 51A, of the Unlawful Activities (Prevention) Act, 1967 (**UAPA**), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated [August 27, 2009](#) detailing the procedure for the implementation of Section 51A of the UAPA. 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.

Accordingly, we need to ensure the effective and expeditious implementation of said Order has been issued vide SEBI Circular ref. no: [ISD/AML/CIR-2/2009 dated October 23, 2009](#), which needs to be complied with scrupulously.