

SANTOSH KUMAR KEJRIWAL SECURITIES PVT LTD

PMLA POLICY

This policy has been prepared pursuant to 'Prevention of money Laundering Act', 2002 (PMLA) as applicable to the intermediary' registered under Section 12 of the SEBI Act,

It provides general background on the subject of money laundering and terrorist financing and summarizes the main provisions of applicable anti money laundering and anti-money terrorist financing legislation in India.

The provisions of PMLA-2002 are applicable for the company. The procedure for the purpose are selected on the basis of specific nature of its business. Organizational structure, type of customers and transaction etc to satisfy itself that the measures adopted by the company are adequate and appropriate to follow the spirit of the suggested measures the Prevention of Money Laundering Act, 2002.

This policy provides to have a system in place to identify, monitor and reporting the suspected money laundering or terrorist financing transactions to law enforcing authorities. This policy are in conformity with SEBI Guidelines, and Exchanges Requirements.

Obligations of intermediaries under Prevention of Money Laundering Act, 2002 (PLMA)

- Appoint a Principal Officer who would be responsible for ensuring of provisions of PMLA
- Name, designation, address and e-mail address of such Principal officer be intimated to Office of Director – FIU, Delhi
- Adopt written procedures to implement the anti-money laundering provisions
- Communicating the policies relating to PMLA/CFT to management/staff handling accounts information, securities transactions and customer records (at branches/ department/ subsidiaries)
- The Policy to contain ; risk based approach, classification of clients as Clients of Special category (CSC), verification of names of customers in updated list of individuals and entities subject to various sanction measures of UN Security Council Committee and complying with Government order UAPA
- Co-operation with law enforcement authorities and timely disclosure of information

The Policy aims to achieve:

- a) Customer acceptance policy and customer due diligence measures

- b) Monitoring of transaction, its evaluation for the purpose.
- c) Maintenance of records.
- d) Compliance with statutory and regulatory requirements
- e) Co-operation with law enforcing agencies, including the timely disclosure of information.
- f) Proper training of the staff member in efficient monitoring the procedure.
- g) Role of internal auditors to ensure compliance of policies, procedures and control to prevent money laundering.

Appointment of Principal Officer:

To prevent and control Money Laundering, we have appointed “Principal Officer” in terms of Money Laundering Act, 2002 and the same were intimated to FIU-DIRECTOR, Chanakyapuri, Delhi.

RIGHTS AND POWERS OF PRINCIPAL OFFICER

1. The principal officer / other appropriate officials have timely access to customer identification data and other CDD information.
2. The principal officer has access and is able to report to Senior Management his/her next reporting level or the Board of Directors.

CONTENTS OF PMLA/CFT GUIDELINES

1. Communicating the policies relating to PMLA/CFT to management/staff handling accounts information, securities transactions and customer records (at branches/ department/ subsidiaries)
2. The above to contain ; risk based approach, classification of clients as Clients of Special category (CSC), verification of names of customers in updated list of individuals and entities subject to various sanction measures of UN Security Council Committee and complying with Government order UAPA.
3. Co-operation with law enforcement authorities and timely disclosure of information.

Risk-Based Approach to KYC

Client acceptance is a critical activity in AML compliance. Every new Client accepted by an institution provides the individual 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 imperative that institutions capture information about their customers’ background, sources of funds, business, domicile and financial

products used by them and how these are delivered to them in order to properly understand their risk profile.

Encouragingly, 88 per cent of respondents reported that they are adopting a risk based approach to account opening, and hence KYC, with another 12 per cent actively considering moving towards it.

With the multitude of requirements by different regulators around the globe, specifically when entering into a correspondent financial relationships, Indian financial institutions may have adopted a risk-based approach earlier than expected and before regulations mandated it. For local business of multinational financial institutions this would not be the case as they often adopt global policies and procedures, hence, they follow global best practices and standards.

As customer risk rating and KYC drives enhanced due diligence and ongoing monitoring it is critical that organizations conduct a comprehensive assessment to understand the risks associated with their business and customers. This in turn will provide a basis upon which associated policies and procedures can be developed.

Across all the sectors, the greatest consideration was the nature of the customer's business. With increased regulatory concern on PEP's, it is surprising to note that they do not constitute the heaviest weightage. In absence of the active review by various industry bodies and independent experts, it is unclear how effective these processes are and if they would meet best practice standards.

We have adopted the following specific parameters, which are related to the overall '*Client Due Diligence Process*':

- a. Policy for acceptance of clients
- b. Procedure for identifying the clients
- c. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)
- d. Risk management
- e. Analyzing alerts
- f. Reporting of alerts to FIU-IND
- g. Other Parameters

(a) Policy for acceptance of clients

We are taking following safeguards while accepting the clients:

1. We have instructed our account opening section not to open account in a fictitious / benami name or on an anonymous basis in any circumstances.
2. It is Necessary made proper 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.
3. We have not been allowing account opening, where it is unable to apply appropriate clients due diligence measures / KYC policies i.e. it is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non cooperation of the Client.
4. We have been regularly updating KYC profile of “clients of special category” defined under Money Laundering Act 2002, if any.
5. We are taking full detail of all the clients including occupational detail and financial detail.
6. We have been properly complying documentation requirement and other information in respect of different classes of clients depending on perceived risk and having regard with the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI and SEBI from time to time.
7. We have not been allowing any client to act on behalf of another person / entity.
8. We have been taking special caution in case of account opening of NRI, OBC, FIIs etc.
9. Special instructions given to update on yearly Basis financial updates of all the clients.

(b) Procedure for identifying the clients

1. Maintenance of updated list of individuals / entities subject to various sanctions / measures available from the site <http://www.un.org/sc/committees/1267/consolist.shtml> and to regularly scan all existing accounts to ensure that no account is held by any of the entities or individuals included in the above list.
2. For customers that are natural persons, it is required to 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, it is required to (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.

3. In the event of matching any particulars of designated individuals/entities, we will inform the full particular of the funds, financial assets or economic resources or related services held in the form of securities, within 24 hours to the joint secretary (IS.I) Ministry of Home Affairs, at a given fax / phone number and email id and will also send the same to the email id and address of SEBI.
4. In the event of matching the details beyond doubt, we will prevent the persons from conducting any further financial transactions under intimation to the above mentioned authorities and will file STR to FIU, IND, covering all transactions.
5. The 'Know your Client' (KYC) policy is clearly defined and adopted under the supervision of Principal Officer.
6. We have been identifying the client by using reliable sources including documents / information, in person verification, etc.
7. We have seen each original document prior to acceptance of a copy and same be stamped "Verified with the original". The information collected by us is enough to satisfy competent authorities (regulatory/ enforcement authorities) in future that due diligence was observed by us in compliance with the Guidelines.
8. We have been noting failure by prospective client to provide satisfactory evidence of identity and same to be reported to the higher authority within the organisation.

(c) Transaction monitoring and reporting especially Suspicious Transactions Reporting

Ongoing monitoring is an essential element of effective KYC procedures. We can effectively control and reduce the risk only if the company 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 pay 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:

1. we will examine the background and the purpose of transactions which are complex or unusually large/ with patterns which appear to have no economic purpose/ which exceed the limits specified for the relevant class of client accounts, and record the findings in writing; make available such findings, records and related documents to auditors, SEBI, Stock Exchanges, FLUIND, other relevant authorities during audit, inspection or as and when required.

2. we will submit cash Transactions Report (CTR) wherever applicable, for each month by 15th of the succeeding month to FIU-IND
3. We will submit Suspicious Transaction Report (STR) within 7 days of arriving at a conclusion that any transaction are of suspicious nature to FIU-IND
4. To preserve records involving CTR/STR for ten years as required under PMLA, 2002
5. We have been taking close surveillance, where transaction amounting to Rs. 10 Lacs or more.
6. We have not been allowing any cash transaction with client.
7. We regularly monitor the transactions for generation of alerts for identification of suspicious transactions.

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

(d) Risk Management

The Board of Directors of the company ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation covering proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibilities are explicitly allocated within the company for ensuring that the Company's policies and procedures are implemented effectively. The company, in consultation with boards, has decided to devise procedures for creating Risk Profiles of the existing and new customers and apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

As The internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures, the compliance function should provide an independent evaluation of the Company's own policies and procedures, including legal and regulatory requirements. The company will appoint and conduct Concurrent/ Internal Audits on specific intervals that will specifically check and verify the application of KYC procedures at the branches and will comment on the lapses observed in this regard. The compliance in this regard may be put up before the Board on quarterly intervals.

The company will conduct an ongoing employee training programme so that all the staff are adequately trained in KYC procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently

Implementation of KYC procedures requires the company to demand certain information from client which may be of personal in nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the client as to the motive and purpose of collecting such information. There is, therefore, the company will educate, from time to time, the customer of the objectives of the KYC programme.

(e) Analyzing alerts

1. We have mechanism to analysis the alerts, as and when generated and also using KYC information including details of occupation and financial status at the time of analyzing alerts.
2. The company will maintain record of all such suspicious transactions, its nature and its value

(f) Reporting of alerts to FIU-IND

1. All the suspicious transaction Alerts generated will be reported to FIU-IND.

(g) Other parameters

➤ **Retention of Records**

We have observed the following document retention:

- a. We have bound to maintain all necessary records, if any, on transactions, both domestic and international at least for the minimum period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.
- b. We have also bound to kept records, if any, on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for the same period.

➤ **Training of staff**

The company has adequately trained staff in AML and CFT (Combating Financing of Terrorism) procedures.

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

Review of PMLA/CFT Procedures

We will review regularly the policy and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness.