

1. FOREWORD:

The Securities and Exchanges Board of India, in order to protect the Securities & commodity derivatives market from the menace of money laundering, felt it necessary to bring the members of commodity exchanges within the reporting ambit of Prevention of Money Laundering Act 2002 (PMLA). The members of the exchanges have, therefore, to follow and adopt:

- The Prevention of Money Laundering Act 2002
- Prevention of Money laundering (Maintenance of records of the nature and value of transaction, the procedure and manner of maintaining and time for furnishing information and verification and maintenance of the identity of clients of the Banking companies, Financial Institutions and Intermediaries) Rules, 2005
- All other rules, regulations, notifications issued by the Government of India from time to time in that behalf.

SEBI's basic objective is that Members have adequate controls and procedures in place so that they know the customers with whom they are dealing.

2. PREAMBLE:

Money Laundering is a serious threat to financial system of all countries and it leads to destruction of the country's sovereignty and character. Financial sector institutions, Banks and Intermediaries remain the primary gateway to the financial system of any country. Once illegal proceeds get into a depository institution, they can be moved instantly by wire or disguised through comingling with legitimate funds. With the advent of Internet and remote banking, depository institutions face increased challenges identifying customers and their customers' sources of funds.

Need for AML Policy:

- To prevent criminal elements from using the Commodities trading system for money laundering activities.
- To enable the broker to know/understand the customers and their financial dealings better, this in turn would help to manage risks prudently.
- To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- To comply with applicable laws and regulatory guidelines.
- To take necessary steps to ensure that the concerned staff is adequately trained in PML procedures.
- Reporting of STRs to FIU as per the guidelines of PML Rules, 2002.

1. 3. Policy of Rikhav Securities Limited

Rikhav has resolved that it would, as an internal policy, take adequate measures to prevent money laundering and shall put in place a frame-work to report cash and suspicious transactions to FIU as per the guidelines of PMLA Rules, 2002.

4. Definitions:

- i. “Money Laundering”: Money Laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds. The term “Money Laundering” is also used when the funds are used for terrorist financing, though the origin of the funds may be legitimate.

This process is often achieved by converting the original illegally obtained proceeds from their original form, usually cash, into other forms such as deposits or securities and by transferring them from one financial institution to another using the account of apparently different persons or businesses.

The process of ML, regardless of its degree of complexity, is accomplished in three stages, namely the placement stage, layering stage and integration stage.

Placement Stage:

The first stage is successfully disposing of the physical cash received through illegal activity. The crooks accomplish this by placing this into traditional or non-traditional financial institutions. This involves the physical movement of the cash proceeds. For most criminal transactions, cash is the most common medium of exchange and criminals who accumulate large volumes of cash are the most vulnerable to detection and seizure. As a result, money launderers will attempt, through placement, to channel the funds into financial institutions.

Layering Stage:

After the funds enter the company, the money launderer will further separate the illicit proceeds from their illegal source through a process of layering. Layering occurs by conducting multiple, complex, financial transactions that make it difficult to link the money to an illegal activity. In this stage he concentrates on separation of proceeds from criminal activity through the use of various layers of monetary transactions. These layers are aimed at wiping audit trails, disguise the origin and maintain anonymity for people behind the transactions.

Integration stage:

The final link in money laundering process is sometimes called the integration stage. This occurs when the laundered or cleaned up money is legitimately brought back into financial systems operated by end user and when it is safe and insulated from enquiry by any agency with a legitimate reason for querying the existence of money. Integration moves the funds back into the economy with the appearance of being normal business earnings. It would become extremely difficult at this point to distinguish between illicit funds and legitimate funds.

Section 3 of the Prevention of Money Laundering Act (PMLA) 2002 defines the Offence of Money Laundering as:

- i. "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of the offence of money laundering."
- ii. "Proceeds of crime" has been defined in Section 2 of the PMLA as the property derived or obtained directly or indirectly by any person, as a result of criminal activity relating to a scheduled offence or the value of such property.
- iii. "Scheduled Offences", as per section 2 of PMLA, are specified in two parts of the schedule to PMLA. The value involved in offences specified in Part B should be Rs.30 lakhs or more.
- iv. "Suspicious transactions": Rule 2(1) (g) of PMLA-2002 defines suspicious transactions as:
A transaction whether or not made in cash which, to a person acting in good faith-
 - (a) Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
 - (b) Appears to be made in circumstances of unusual or unjustified complexity; or
 - (c) Appears to have no economic rationale or bona-fide purpose; or
 - (d) Gives rise to a reasonable ground of suspicion that it may involve financing of activities relating to terrorism.
- v. 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 company;
 - One on whose behalf the account is maintained (i.e., the beneficial owner);
 - Any person or entity connected with a financial transaction which can pose significant reputational or other risks to the company.
- vi. Financial Intelligence Unit (FIU) – INDIA

It is an independent body to report directly to the Economic Intelligence Council (EIC) headed

by the Finance Minister; FIU-IND has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

5. Implementation of this Policy:

Mr. Hitesh Lakhani is the Designated Director appointed for PMLA.

Mr. Vishal Patel is the Principal Officer responsible for compliance of the provisions of the PMLA and AML Guidelines act as a central reference point and play an active role in identification & assessment of potentially suspicious transactions. Ensure that Rikhav discharges its legal obligation to report suspicious transactions to the concerned authorities.

6. CUSTOMER DUE DILIGENCE PROCESS – Securities & DP Activities

The main aspect of this policy is the Customer Due Diligence Process which means:

- Obtaining sufficient information about the client in order to identify who is the actual beneficial owner or on whose behalf transaction is conducted.
- Verify the customer's identity using reliable, independent source document, data or information.
- Conduct on-going due diligence and scrutiny of the account/client to ensure that the transaction conducted are consistent with the client's background/financial status, its activities and risk profile.

The Customer Due Diligence Process includes four specific parameters:

- Policy for Acceptance of Clients
- Client Identification Procedure
- Monitoring of transactions
- Tracking and reporting Suspicious Transactions

1. CUSTOMER(CLIENT) ACCEPTANCE POLICY

M/S RIKHAV SECURITIES LIMITED

“PREVENTION OF MONEY LAUNDERING ACT”

Each client should be met in person	<ul style="list-style-type: none"> • Accept client whom we are able to meet personally. Either, the client should visit the office/branch or concerned official may visit the client at his residence / office address to get the necessary documents filed in and signed. • Preferably accept clients who live within the jurisdiction of the branch. • As far as possible, ensure that the new client is introduced by an existing client. In case client is not introduced by an existing client, then the employee who visits the client/ meets the client in person shall verify and sign as introducer. The employee meeting the client does in-person verification and sign as introducer in the form by specifying the name, employee code, designation, branch and department serving.
Accepts clients on whom we are able to apply appropriate KYC procedures	<ul style="list-style-type: none"> • All supporting documents and complete information as specified by SEBI and Commodity Exchanges should be obtained from the client and the same shall be verified against the original documents without any exceptions. • Ensure that the “Know Your Client” guidelines are followed without any exception and that the initial forms taken by the clients are filled in completely.
Do not accept clients with identity matching persons known to have criminal background	Check whether the client’s identity matches 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/regulatory agency worldwide.
Be careful while accepting Clients of Special category	<ul style="list-style-type: none"> • We should be careful while accepting and properly scrutinize the records / documents pertaining to clients belonging to below mentioned categories: - <ul style="list-style-type: none"> ○ clients of special category like HNIs, Trust, Charities, NGOs, Politically Exposed Persons (PEP), persons of foreign origin; ○ companies having closed share holding/ ownership, companies dealing in foreign currency, shell companies, overseas entities, clients in high risk countries, non face to face clients, clients with dubious background. ○ Current/Former Head of State, Current/ Former senior high profile politician, Companies offering foreign exchange, etc.) ○ Clients from high-risk countries (like Libya, Pakistan, Afghanistan, etc.) or clients belonging to countries where corruption/ fraud level is high (like Nigeria, Burma etc).
Do not accept client registration forms which are suspected to be fictitious	Ensure that no account is being opened in a fictitious / benami name or on an anonymous basis.
Do not compromise on submission of: (i) Mandatory	(i) Client’s account should be opened only on receipt of mandatory information along with authentic supporting documents as per the regulatory guidelines. Do not open the accounts where the client

information/ documents	refuses to provide information/documents and we should have sufficient reason and record to reject the client's request towards this reluctance
(ii) Financial Details	(ii) Client's account should be opened only on receipt of financial details along with supporting documents, like ITR, Copy of Annual Accounts, Copy of Form 16 in case of salaried employees, Salary Slip, Net worth certificate signed by CA, Bank account statement for last 6 months, Self declaration along with relevant supporting documents.

II. CUSTOMER (CLIENT) IDENTIFICATION PROCEDURE

Objective: To have a mechanism in place to establish identity of the client along with firm proof of address to prevent opening of any account which is fictitious / benami / anonymous in nature.

Documents which can be relied upon:

- PAN Card: PAN card is mandatory and is most reliable document as only one card is issued to an individual and we can independently check its genuineness through IT website.
- IDENTITY Proof: PAN Card itself can serve as proof of identity. However, in case PAN card carries an old photograph of the holder, which does not match current facial features of the client, we should take other identity proof in form of Voter's Identity card, Passport, Ration Card or any Government/PSU/Bank issued photo identity card.
- ADDRESS Proof: For valid address proof we can rely on Voter's Identity Card, Passport, Bank Statement, Ration card and latest Electricity/telephone bill in the name of the client.

DOCUMENTS TO BE OBTAINED AS PART OF CUSTOMER IDENTIFICATION PROCEDURE FROM NEW CLIENTS:

1	In case of individuals, one copy of the following documents have to be obtained	<ul style="list-style-type: none"> • As PAN is mandatory, verify its genuineness with IT website and cross verify the PAN card copy with the original. [Please put "verified with original" stamp as proof of verification] • Other proofs for identity are Voter's Identity card, Passport, Ration Card or any Government/PSU /Bank issued photo identity card or any other document prescribed by the regulatory authorities. • Address proof in the form of Voter's Identity Card, Passport, Bank Statement, Ration card and latest Electricity/telephone bill in the name of the client or any other document prescribed by the regulatory authorities.
2	In case of corporate, one certified copy of the	<ul style="list-style-type: none"> • Copy of the Registration/Incorporation Certificate • Copy of the Memorandum & Articles of the Association

	following documents must be obtained	<ul style="list-style-type: none"> • Copy of the PAN card and the Director Index No. (DIN) • Copy of the latest audited Annual Statements of the corporate client • Latest Net-worth Certificate • Latest Income Tax return filed. • Board Resolution for appointment of the Authorised Person(s) who will operate the account. • Proof of address and identity of Authorized Person(s)
3	In case of partnership firm one certified copy of the following must be obtained	<ul style="list-style-type: none"> • Registration certificate • Partnership Deed • PAN card of partners • Authorization letter for the person authorized to open and operate the account • Proof of identity and address of the authorised person. • Annual statement/returns of the partnership firm
4	In case of a Trust, one certified copy of the following must be obtained	<ul style="list-style-type: none"> • Registration certificate • Trust Deed • PAN card • Authorization letter for the entity authorized to act on their behalf • Officially valid documents like PAN card, voters ID, passport, etc of person(s) authorized to transact on behalf of the Trust.

IDENTIFICATION OF ULTIMATE BENEFICIAL OWNERSHIP:

Beneficial ownership will be determined as under:-

For clients other than individuals or trusts:

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

- 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:

- a. More than 25% of shares or capital or profit so the juridical person, where the juridical person is a company;
- b. More than 15% of the capital or profit so the juridical person, where the juridical person is a partnership; or
- c. More than 15% of the property or capital or profit so 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, the identity of the relevant natural person who holds the position of senior managing official needs to be obtained.

For client which is at rust:

- Where the client is a trust, the intermediary shall identify the beneficial owner so the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

GENERAL GUIDELINES

1. Always check original documents before accepting the copies.
2. Obtain the latest photograph of account holder/ authorized person(s).
3. Check for latest IT return of the client/ Net worth Certificate for ascertaining the financial status of the client to know the client suitability of the product being sold to the client. Review the above details on-going basis to ensure that the transactions being conducted are consistent with our knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.
4. Scrutinize the forms submitted by the client thoroughly and cross check the details with various documents obtained like source of income. If required, ask for any additional details like salary slips, etc. to satisfy yourself whenever there is a doubt.
5. Keep watch on the welcome kits returned with reason - undelivered. Officials from Head Office should be alerted, client be contacted immediately on telephone and the trading, if suspected, should be suspended. If Employee of Rikhav Group introduces the client, exact relation of the client with such employee should be documented.
6. For scrutiny / back ground check of the Franchisee, websites such as www.watchoutinvestors.com should be referred. Also, Prosecution Database / List of Vanishing Companies available on www.cdslindia.com; www.bseindia.com; www.nseindia.com; www.mcxindia.com; www.icex.com; www.sebi.gov.in

DOCUMENTS TO BE OBTAINED AS PART OF CUSTOMER IDENTIFICATION PROCEDURE
For all EXISTING CLIENTS:

On an on-going basis, the branches should ensure that the details given in the KYC, by the client, match with the current details of the client. If required, we can seek additional documents/information from the client to verify the financial/general status of the client.

In cases where:

- There is any material negative change in the financial details of the client from what is given in the KYC
- If the client is not contactable/traceable or contracts notes/ communications sent are received back undelivered
- In case the client is prohibited by any regulatory authority
- The client refuses to provide additional information/document asked for
- There is a material change in the mandate holder profile/details

Branches should immediately bring the same to the notice of the Principal Officer to decide on the necessary course of action, including reporting to FIU, New Delhi.

Customer Identification modus operandi:

Customer identification is an essential element of KYC standards. A customer would include the person or entity that maintains an account with the Member/intermediary or those on whose behalf an account is maintained (i.e., beneficial owners). Members should undertake the following processes for proper identification of customers:

- i) Identifying the customer and verifying that customer's identity using reliable, independent source documents;
- ii) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the Member is satisfied that it knows who the beneficial owner is;
- iii) In case of high value of transactions, obtaining information on the purpose and intended nature of the business relationship;
- iv) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Member's knowledge of the customer,

their business profile and risk profile, including, where necessary, the source of funds.

KYC and Risk Profile of the Customers:

We should accept the clients based on the risk they are likely to pose. The aim is to identify clients who are likely to pose a higher than average risk of money laundering or terrorist financing. For this purpose, we need to classify the clients as Low Risk, Medium Risk and High Risk clients. By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for High Risk client we have to apply higher degree of due diligence. The factors of risk perception depend on client's location, nature of business activity, turnover, nature of transaction, manner of payments, etc.

In order to achieve this objective, all clients of the branch should be classified in the following category:

- Category A – Low Risk
- Category B – Medium Risk
- Category C – High Risk

Category A clients are those pose low risk. They are Individuals/ HNIs who have a respectable social and financial standing. These are the clients who make payment on time and take delivery of shares.

Category B clients are those who are intra-day clients or speculative clients. Account with status as Minor being operated by their guardians

Category C clients are those who have defaulted in the past, have suspicious back ground, do not have any financial status, Corporate accounts. NRI accounts etc.

We have to be careful while monitoring the transactions of B and C category clients.

Any change in the risk profile of the client/mandate holder, has to be ascertained by the concerned branch official and be reported to the Head Office immediately.

- 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, Government departments and Government owned companies, regulators and statutory bodies etc.

For the **High risk** profiles; high risk customers would include the following:

- Companies having close family shareholdings or beneficial ownership
- Non-face-to-face clients

- Non-resident clients
- High net worth clients,
- Trusts, Charities, NGOs and organizations receiving donations
- Politically exposed persons (PEP) of foreign origin
- 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 which are perceived to be sponsors of international terrorism, offshore financial centres, tax havens, countries where fraud is highly prevalent)
- Clients with dubious reputation as per public information available

The decisions to enter into business relationships with high risk customers, such as politically exposed persons, should be taken exclusively at senior management level only.

Mandate Holder Policy

- The primary objective of this policy is to ensure that we are aware as to who is the ultimate beneficiary of the transaction and that the transactions executed, through the mandate holder, are bonafide.
- It is possible that some of the individual clients might appoint a mandate holder. Normally the trading account is opened in the name of various family members and one the family member will hold the mandate.
- Whenever any account is operated by a mandate holder, find out the relationship of the mandate holder with the client, followed by establishing the identity of the mandate holders by obtaining proof of identity and address.
- Do not accept any payment from the account of mandate holder in favour of the client. All the payments have to be received from the client's bank account only for which the PoA holder may or may not have the mandate to operate the bank account. Similarly pay-out cheques should be issued only in the name of the client and not in the name of the mandate holder.

In case there is suspicion on the relationship between the mandate holder and the actual client or in case behaviour of the mandate holder is suspicious, do take necessary advice from the Head Office officials.

TRANSACTION MONITORING

Transaction monitoring is an extremely important aspect of the risk profiling system. Whenever the RMS Team sees that a client is doing or having an unusual or auspicious trading pattern also from the same dashboard sees the income and networth of the client along with

risk level and the special category if any one of the scenarios, then he or she could immediately upgrade the risk of the client from Low to medium or from medium to high.

This risk allocation will happen through the alerts downloaded by our back office software immediately and the RMS team member does not need any approval to do so.

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

Parameters available on the Reports: Following are the parameters /nature of alerts /reports / scenarios available for securitization.

Alert 1: Fund flow

This parameter tells you the financial size vis a vis the fund flow and this will cover inflow and out flow of funds.

It will highlight client's who are bringing funds way beyond their financial strength.

Alert 2: Client Concentration

- To understand whether a given client is focusing on a particular commodity over a period of one year or x period. Also analysis of his focus on the investment pattern.
- Could give lead to Insider Trading indicators
- Could give lead to an understanding that for multiple accounts there is a common operator based on trading pattern
- Could give lead to an understanding that for multiple accounts there is a common operator based on mobile number or email address

Alert 3 : Illiquid commodities

To understand the intent of the client when he would like to deal in not so liquid commodity. This could lead to indicator so unusual activity or manipulation activity in illiquid commodity. We will block these commodities from trading.

Alert 4 : Key person matching for Non Individuals

These criteria will highlight to you accounts which have common controllers or common owners. Example if an Individual is a director in 4 different private limited companies and they have 4 trading account with the broker.

The matching is done based on

- Name of the Individual
- Email of the Individual
- PAN of the Individual
- Mobile Number if the Individual

Alert5:Crossdeals

We generate cross deals report to examine whether any unusual transactions are taking place.

Alert 6 : Activity in dormant account

We are generating this alert to examine if any unusual trading activities taking place. We take reactivation letter from client before allowing any trading in dormant account.

7. Reporting of Transactions

Reporting of Transaction to Financial Intelligence Unit-India:

In terms of the PMLA rules, Intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit- India (FIU-IND)

- I. **Cash Transaction Reports:** The Prevention of Money-laundering Act, 2002, and rule there under require every intermediary, to furnish to FIU-IND information relating to:
- 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;

The cash transaction report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month.

All are requested not to accept cash from the clients whether against obligations or as margin for purchase of commodities or otherwise. All payments shall be received from the clients strictly by account payee crossed cheques drawn in favour of Rikhav Securities Ltd.

In case account payee cheques have been received from a bank account other than that captured in records the same can be accepted after ascertaining that the client is the first holder of the account. Relevant copies of the supporting documents should be sent to HO and details of such accounts should be captured in records.

Only in exceptional cases, bank draft/pay-order may be accepted from the client provided identity of remitter/purchaser written on the draft/pay-order matches with that of client else obtain a certificate from the issuing bank to verify the same.

All cash transactions are required to be reported on monthly basis to the Principal Officer by each branch/Sub-broker by 7th of the following month.

II. Suspicious Transaction Reports:

All are requested to analyze and furnish details of suspicious transactions, whether or not made in cash. It should be ensured that there is no undue delay in analysis and arriving at a conclusion.

The intermediary shall furnish to FIU-IND information of all suspicious transactions whether or not made in cash.

The Principal Officer should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion. The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND. Utmost confidentiality should be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.

What is a Suspicious Transaction: 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 circumstance of unusual or unjustified complexity; or
- Appears to have no economic rationale or bona fide purpose
- Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Reasons for Suspicion:

- Identity of client
 - False identification documents
 - Identification documents which could not be verified within reasonable time

- Non-face to face client
- Clients in high-risk jurisdiction
- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities
- Receipt back of well -come kit undelivered at the address given by the client.
- Suspicious Background
 - Suspicious background or links with criminals
- Multiple Accounts
 - Large number of accounts having common parameters such as common partners / directors / promoters / address/ email address / telephone numbers introducer or authorized signatory.
 - Unexplained transfers between such multiple accounts.
- 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
- Nature of Transactions
 - Unusual or unjustified complexity
 - No economic rationale or bonafied purpose
 - Source of funds are doubtful
 - Appears to be case of insider trading

- Purchases made on own account transferred to a third party through an off market transactions through DP account
- Transactions reflect likely market manipulations
- Suspicious off market transactions
- 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 client's apparent financial standing
 - Inconsistency in the payment pattern by client

What to Report

- 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 reason of suspicion.

When to Report

In terms of the PMLA rules, brokers and sub-brokers are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) 6th Floor, Hotel Samarat, Chanakyapuri, New Delhi - 110021 as per the schedule given below:

<u>Report</u>	<u>Description</u>	<u>Due Date</u>
CTR	All cash transactions of the value of more than Rs.10 Lakhs or its equivalent in foreign currency All series of cash transactions integrally connected to each other which have been valued below Rs.10 Lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month	15th day of the succeeding month

CCR	All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions*	Not later than seven working days from the date of occurrence of such transaction*
STR	All suspicious transactions whether or not made in cash	Not later than seven working days on being satisfied that the transaction is suspicious

In view of the same, Head office officials are required to collect information from the Branches/Departments/Sub-brokers under their control/ jurisdiction and submit report to the Principal Officer on Cash transactions on monthly basis, by the 15th day of the following month and suspicious transactions within three working days of establishment of such transaction to enable the Principal Officer to report the same to the Director, Financial Intelligence Unit-India (FIU-IND) within the stipulated time.

Other Important Points

- Reasons for treating any transaction or a series of transactions as suspicious should be recorded. It should be ensured that there is no undue delay in arriving at such a conclusion.
- Utmost confidentiality should be maintained in submitting the information.
- The reports may be transmitted by email/speed/registered post/fax at the Head Office addressed to the Principal Officer.
- No restriction may be put on operations in the accounts where a Suspicious Transaction Report has been made.
- It should be ensured that there is no tipping off to the client at any level.

8. Principal Officer and Designated Director

In case any further information /clarification is required in this regard, the "Principal Officer" or "Designated Director" may be contacted. Details mentioned as under:

Principal Officer:

Name: Mr. Vishal Patel

Address:*M/s. Rikhav Securities Ltd.**34/35/36/38, MATRUCHHAYA, 4TH FLOOR, SAROJINI NAIDU ROAD,
MULUND WEST, MUMBAI-400080**Email Id: vishal@rikhav.net***Designated Director:***Name: Mr. Hitesh Lakhani***Address:***M/s. Rikhav Securities Ltd.**34/35/36/38, MATRUCHHAYA, 4TH FLOOR, SAROJINI NAIDU ROAD,
MULUND WEST, MUMBAI-400080**Email Id: hitesh@rikhav.net***9. 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. The obligations to be followed by intermediaries 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.

10. CUSTOMER EDUCATION/ EMPLOYEE'S TRAINING/ EMPLOYEE'S HIRING

Customer Education - Implementation of KYC procedures requires Rikhav to demand certain information from customer which may be of personal nature or which has hithert on ever been called for. This sometimes leads to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Relationship Managers of Rikhav shall be trained to explain to the customers the regulatory requirements and benefits of adhering to the KYC guidelines and seek co-operation of the customer.

Employees' Training – Rikhav shall have an ongoing employee training programme so

Employees' Training – Rikhav shall have an ongoing employee training programme so that the members of the staff are adequately trained in KYC / AML procedures and fully understand the rationale behind the KYC/AML policies and implement them consistently.

Hiring of Employees – KYC norms / AML standards / CFT measures have been prescribed to ensure that criminals are not allowed to misuse our infrastructure. It should therefore, be necessary that adequate screening mechanism is put in place by Rikhav as an integral part of the recruitment / hiring process of personnel.

Retention of Records

Intermediaries shall take appropriate steps to evolve an internal mechanism for proper maintenance and preservation of such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of Eight years from the date of transactions between the client and intermediary.

As stated in sub-section 2.2.5, intermediaries are required to formulate and implement the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. 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 Eight years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

Thus the following document retention terms shall be observed:

- a) All necessary records on transactions, both domestic and international, shall be maintained at least for the minimum period prescribed under the relevant Act and Rules (PMLA and rules framed thereunder as well SEBI Act) and other legislations, Regulations or exchange bye-laws or circulars.
- b) Registered intermediaries shall maintain and preserve the records of documents evidencing the identity of its clients and beneficial owners (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence for a period of Eight years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

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

Records of information reported to the Director, Financial Intelligence Unit – India (FIU – IND)

Registered Intermediaries shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, for a period of Eight years from the date of the transaction between the client and the

intermediary.

List of Designated Individuals/ Entities

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/sc/committees/1267/consolist.shtml>. Registered intermediaries are directed to ensure that accounts are not opened in the name of anyone whose name appears in said list. Registered intermediaries shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list. Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to SEBI and FIUIND.

11. REVIEW OF PMLA POLICY

This policy will be reviewed on yearly basis or any regulatory changes whichever is earlier. There view of the policy will be carried out by a person other than involved in framing the policy.



Place : Mumbai
Date : 21/08/2021