

ANTI MONEY LAUNDERING POLICY

CHUKNOO SECURITIES LIMITED

**Regd Office- 311-318, Krishna Tower,15/63
Civil Lines Kanpur-208001**



Compliance Officer: Mr. Yash Agarwal

Principal Officer: Mr. Rajeev Tulsian

The Policy is reviewed on a Annual basis

Date of Last Review-01-04-2018

Chuknoo Securities Ltd

Policies and Procedures to combat money laundering and terrorist financing

Pursuant to the provisions of the Prevention of Money Laundering Act, 2002(PMLA) which was published in the gazette of India on 1st July 2005 every banking financial and non banking financial companies and financial intermediaries ,which includes stock brokers have to formulate internal polices and procedures to guard against money laundering activities. Our company CSL, being a member of NSE and BSE is a financial intermediary and hence should put in place such policies and procedures as per the provisions of the above said act and should maintain a record of all the transaction as prescribed under the rules framed under PMLA which include :

- All cash transactions of the value of more than Rs 10 lacs 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 take place within one calendar month.
- All suspicious transactions (including all transactions i.e. those integrally connected and those remotely connected) whether or not made in cash and including, inter-alia, credits or debits into from any non monetary account such as d-mat account, security account maintained by the registered intermediary.

As per the provisions of the Act, it is also incumbent on the company to have the internal procedures as stated above reduced to writing. It is hence that these procedures were for implemented by Chuknoo Securities Ltd.

Procedures

As per the guidelines issued under the provisions of the PMLA each stock broker should have procedures for Client Due Diligence process which include

- (a) Policy for acceptance of client
- (b) Procedure for identifying clients and
- (c) Transactions monitoring and reporting especially suspicious transaction reporting.

1.1 Client Due Diligence Process-General

This consist of the following

- ✓ Ensure that KYC Norms are strictly followed and all the information provided in the KYC form are obtained and filled up.
- ✓ Obtain sufficient information in order to identify persons who beneficiary own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. The beneficial owner is 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.

- ✓ Verify the customer's identity using reliable, independent source documents, data or information.
- ✓ Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted.
- ✓ Verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and
- ✓ 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 customer, its business and risk profile, taking into account, where necessary, the customer's source of funds

Reliance on third party for carrying out Client Due Diligence (CDD)

Registered intermediaries may rely on a third party for the purpose of (a) identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

Such reliance shall be subject to the conditions that are specified in Rule 9 of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. Further, it is clarified that the registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable

1.2 Policy for Acceptance of Clients

The policy is to enable customer due diligence on a risk sensitive basis depending on the type of customer business relationships or transactions. Accordingly the following safeguards are to be followed while accepting the clients.

1.2.1 No account is opened in a fictitious/benami name or on an anonymous basis

1.2.2 Risk Perception :

Based on client's location, nature of business activity, trading turnover, manner of making payment for transactions undertaken, clients should be classified into low, medium and high risk category. Though as per guidelines issued by SEBI and practiced by the company this system of making payments to and for receiving payments from, clients is through banking channels only and in the manner specified, the following points are to be ensured.

(a) No payment in cash is either accepted or made to the client.

(b) Display this clearly in the notice board and as part of Do's and Don'ts' issued in writing to the clients as part of client registration.

(c) Discourage payment by clients by DD. In exceptional cases DD's may be accepted if the same is supported by a letter from the client to the effect that the DD is from the banking account ,proof of which is provided to the company.

(d) Ensure that the internal control policies in this regard are strictly followed.

1.2.3 Ensure that no account is opened where the intermediary is unable to apply appropriate clients due diligence measures / KYC policies. Such cases are where:

(a) It is not possible to ascertain the identity of the client

(b) Information provided is suspected to be non genuine.

(c) It appears that client's does not co-operate by providing full and complete information

1.2.4 Except in cases where the client and the person who acts for the client are identified or where the company has knowledge about the client and or the person acting for the client, no person shall be permitted to act for and on behalf of a client and where such permission is given ensure the following.

(a) Ascertain that the circumstances which warrant a person to act on behalf of a client is genuine. (Such as prolonged illness (where clearly proved) long absence from station or other genuine in capabilities).

(b) There is proper authorization in favor of the person acting on behalf of the client (Proper POA together with the photograph of the client and the person acting on behalf of the client affixed on POA, which is notarized).

(c) In what manner account should be operated, what limits can be provided the right & responsibilities of the client and the POA holder, etc., are clearly mandated in POA.

1.2.5 Ensure that identity of the client does not match with any person having known criminal background or is not banned in any other manner.

1.2.6. The following are considered as special category clients and in respect of all them utmost care should be taken to clearly identify the client before the account is opened. The category of clients referred to herein are: -

(a) Nonresident clients

(b) High net worth clients

(c) Trust, Charities, NGOs and organizations receiving donations

(d) Companies having close family shareholdings or beneficial ownership

(e) Politically exposed persons (PEP) of foreign origin

(f) Current / Former Head of State, Current or Former Senior High profile politicians and connected persons)

(g) Companies offering foreign exchange offerings

1.2.7 As far as possible reference and confidential report about the genuinity of the client should be obtained from the client's bankers in respect of all cases other than (e),(g)

1.2.8 In respect of those listed as (e), (g) avoid dealing with them and do not open any account for them.

1.2.9 As far as possible and except where it is unambiguously made known that the voluntary donations and other receipts of the Trust/Charitable Organizations/NGO are from genuine sources and not from unidentified or fictitious person, no account of

trust/charitable organization/NGO should be opened.

2. Client Identification Procedure :

- 2.1 Ensure the 'Know your Client' (KYC) policy spelt out in the internal control policy is strictly carried out at different stages i.e. While establishing the intermediary - client relationship, while carrying out transactions for the client or when there arise has doubts regarding the veracity or the adequacy of previously obtained client identification data.
- 2.2 Ensure that the client is identified by using reliable sources including documents / information. Also obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
- 2.3 Ensure that each original document is seen prior to acceptance of a copy.
- 2.4 Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority within the company.
- 2.5 Ensure to maintain continuous familiarity and follow-up where inconsistencies in the information provided by the client are noticed.

Politically Exposed Person (PEP):

- a) Ensure adequate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPS.
- b) All registered intermediaries are required to obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, registered intermediaries shall obtain senior management approval to continue the business relationship.
- c) Registered intermediaries shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP".
- d) The client shall be identified by the intermediary by using reliable sources including documents / information. The intermediary shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
- e) The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
- f) Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within the intermediary.
- g) Every PEP account shall be opened only after approval from higher authority i.e Approval to be taken from senior management/directors.

3. Record Keeping :

3.1 Ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

3.2 Ensure that 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 are maintained

3.3 Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, it is ensure that the following information as regards the accounts of the customers is retained in order to maintain a satisfactory audit trail.

(a) The beneficial owner of the account;

(b) The volume of the funds flowing through the account; and

(c) For selected transactions

(d) The origin of the funds.

(e) The form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;

(f) The identity of the person undertaking the transaction;

(g) The destination of the funds;

(h) The form of instruction and authority.

3.4 Ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. (e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.)

4. Retention of Records

4.1 The following document retention procedure should be observed:

(a) All necessary records on transactions, should be maintained at least for a minimum period of 5 years

(b) Records 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 should also be kept for the same period.

4.2 In situations where the records relate to on-going investigations 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.

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

5. Monitoring of transactions

5.1 Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money Laundering procedures. To achieve this, watch periodically the normal activity of the client so that deviations in transactions / activities are identified and enquired with the client.

5.2 Ensure that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate legal authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department in the Company.

5.3 Ensure that random examinations of selected transactions undertaken by clients are carried out in order to comment on their nature i.e. whether they are the suspicious transactions or not

6. Suspicious Transaction Monitoring & Reporting

6.1 Ensure to take appropriate steps to enable suspicious transactions be recognized and report suspicious transactions. A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

- a) Clients whose identity verification seems difficult or clients appears not to cooperate
- b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
- c) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or their clients based in high risk jurisdictions;
- d) Substantial increases in business without apparent cause;
- e) Unusually large cash deposits made by an individual or business;
- f) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- g) Transfer of investment proceeds to apparently unrelated third parties;
- h) Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of exportimport of small items.

6.2 Any suspicious transaction should be immediately notified to the Money Laundering Control Officer or any other designated officer within the Company. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature reason for suspicion etc. It should however, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

Records of information reported to the Director, Financial Intelligence Unit - India (FIU-IND):
Registered intermediaries shall maintain and preserve the record 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, for a period of five years from the date of the transaction between the client and the intermediary

7.Risk Assessment and List of Designated Individuals/Entities.

Registered intermediaries shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions.

The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required

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> and <http://www.un.org/sc/committees/1988/list.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 FIU-IND.

8. 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.

9. Designation of an officer for reporting of suspicious transactions

7.1 The principal officer already appointed for the purpose should 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

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

8.1. Ensure that adequate screening procedures are in place to ensure high standards when hiring employees. Key positions within the own organization structure should be identified having regard to the risk of money laundering and terrorist financing and the size of their business and ensure that the employees taking up such key positions are suitable and competent to perform their duties. Provide proper antimoney laundering and anti-terrorist financing training to their staff members.

11. Appointment of a Designated Director

- i. In addition to the existing requirement of designation of a Principal Officer, the registered intermediaries shall also designate a person as a 'Designated Director'. In terms of Rule 2 (ba) of the PML Rules, the definition of a Designated Director reads as under:

“Designated Director means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes —

(i) the Managing Director or a Whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,

(ii) the managing partner if the reporting entity is a partnership firm,

(iii) the proprietor if the reporting entity is a proprietorship concern,

(iv) the managing trustee if the reporting entity is a trust,

(v) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and

(vi) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above."

ii. In terms of Section 13 (2) of the PML Act (as amended by the Prevention of Money-laundering (Amendment) Act, 2012), the Director, FIU-IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of the intermediary to comply with any of its AML/CFT obligations.

iii. Registered intermediaries shall communicate the details of the Designated Director, such as, name, designation and address to the Office of the Director, FIU-IND

For Chuknoo Securities Limited

**Rajeev Tulsian
(Principal Officer)**