

Guidelines

On

Anti-Money Laundering Standards

**[Prevention of Money Laundering Act, 2002
(PMLA)]**

R.K. Stockholding (P) Ltd.

Introduction of R.K. Stockholding (P) Ltd.

R. K. Stockholding (P) Ltd. (RKSTOCK) is a member of National Stock Exchange, Bombay Stock Exchange and Metropolitan Stock Exchange of India Ltd. Limited (MSEI) having SEBI Regn No.INZ000211932. GCML is also a depository Participant of CDSL vide DP ID: 41800.

This Anti-Money-Laundering (AML) policy has been prepared in accordance Prevention of Money Laundering Act, 2002 (PMLA Act). This policy also takes into account the provisions of PMLA Act, Master circular issued by SEBI on July 04, 2018 and rules laid down by FIU.

Section 1: Overview

Introduction & Background of AML

The Government of India has serious concerns over money laundering activities which are not only illegal but anti-national as well. Money laundering is the process by which large amount of illegally obtained money (from drug trafficking, terrorist activity or other serious crimes) is given the appearance of having originated from a legitimate source. All crimes that produce a financial benefit give rise to money laundering.

Introduction

1. The provisions of the anti-money laundering and anti-terrorist financing legislation in India and provide details guidance on the practical implications of the Act. The AML sets out the steps that a registered intermediary or any of its representatives, should implement and take action to discourage and identify the money laundering or terrorist financing activities. The relevance and usefulness Guidelines will be kept under review and amend from time to time as per changing requirement.
2. Guidelines are intended for use primarily by Company and it is recognized that a “one-size-fits-all” approach may not be appropriate for the securities industry in India, each registered intermediary should consider the specific nature of its business, organizational structure, type of customers and transactions, etc. when implementing the suggested measures and procedures to ensure that they are effectively applied. The overriding principle is that they should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and the requirements as enshrined in the Prevention of Money Laundering Act, 2002. (PMLA)

As a market participant it is evident that strict and vigilant tracking of all transactions of suspicious nature required.

The prevention of money laundering act, 2002 (PMLA) has been brought into force with effect from 1st July 2005. Necessary notification / rules under the said act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, and Government of India.

Accordingly our company has laid down the following policy guidelines:

Principal Officer:

Mr. Alok Kumar Jamuar is appointed as the Principal Officer. He will be responsible for implementation of internal controls & procedures for identifying and reporting any suspicious transaction or activity to the concerned authorities. Principle officer has the right of timely access to customer identification data, other CDD information and is able to report the same to senior management or the board of directors.

Designated Director

Mr. Navdeep Varshney is appointed as designated director.

Purpose & Scope:

As a Financial Market Intermediary we need to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Accordingly all the back office and trading staff is instructed to observe the following safeguards:

- 1 No Cash transactions for trading in securities shall be allowed from any client in the normal course of business.
- 2 Maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules notified under the PMLA. Such transactions include:
 - 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 take place within one calendar month.
 - All transaction involving receipts by non-profit organizations of value more than rupees ten lakhs or its equivalent in foreign currency.
 - All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non monetary account such as Demat account, security account maintained by the registered intermediary.
- 3 Frequent off Market transfers from one BO account to another shall be scrutinized and asked for. In absence of valid reason case or found suspicious, it shall be brought to the notice of Principal Officer.
- 4 Trading beyond ones declared income: The turnover of the clients should be according to their declared means of income. Any abnormal increase in client's turnover shall be reported to Principal Officer. The Back Office staff should take due care in updating the clients' financial details and shall periodically review the same.

Policies and procedures to combat Money Laundering cover:

- a) The Communication of group policies relating to prevention of money laundering and terrorist financing to all management and relevant staff of the company that handle account information, securities transactions, money and customer records etc. whether in branches, departments;
- b) Customer acceptable policy and customer due diligence measures, including requirements for proper identification;
- c) Maintenance of records;
- d) Compliance with relevant statutory and regulatory requirements;
- e) Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and

- f) Role of internal audit or compliance function to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.

Section 2: Written Anti Money Laundering Procedures

Vision towards Anti Money Laundering

- R. K. Stockholding (P) Ltd (RKSHPL) 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 suspicious transactions to FIU as per the guidelines of PMLA Rules, 2002 and as prescribed by SEBI vide its Circular No. SEBI/HO/MIRSD/DOS3/CIR/P/2018/104 dated July 04, 2018.
- RKSHPL does not deal in cash except in Depository division, where client makes payment of small amount for Annual maintenance of Depository account and other transaction charges; normally amount is Rs.500 or Rs.5000. Hence the requirement of maintaining record of cash transaction in excess of Rs.10 Lakh is ruled out.
- For suspicious transactions whether or not made in cash, we observe the trading pattern of the client on difference criteria like quality of scrip, market participation, Income & Networth, funds received, trading behaviour etc.
- Compliance department of RKSHPL review & update AML policy on time to time based on the circular issued by regulator in consultation with Principal Officer.

The management of our company has formulated and adopt written procedures to implement the anti money laundering provisions as envisaged under the Anti Money Laundering Act. Such procedures as include inter alia, the following specific parameters which are related to the overall 'Client Due Diligence Process':

- Policy for acceptance of clients
- Procedure for identifying the clients
- Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

Client identification procedure:

The 'Know your Client' (KYC) Policy: -

a) While establishing the intermediary – client relationship

- No account shall be opened unless all the KYC Norms as prescribed from time to time by the SEBI / Exchanges are duly complied with, all the information as required to be filled in the KYC form (including financial information, occupation details and employment details) is actually filled in and the documentary evidence in support of the same is made available by the client. Moreover all the supporting documents should be verified with originals and client should sign the KYC & MCA in presence of our own staff and the client should be introduced by an existing clients or the known reference.
- The information provided by the client should be checked though independent source namely.

- Pan No must be verified from Income Tax We Site
- Address must be verified by sending Welcome Letter / Qly Statement of Account, and in case any document returned undelivered the client should be asked to provide his new address proof before doing any further transaction.
- We must exercise additional due diligence in case of the **Clients of Special Category** which include but not limited to :-
 - i. Non-resident clients
 - ii. High-networth clients
 - iii. Trust, Charities, 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. The additional norms applicable to PEP as contained in the subsequent para 2.2.5 of this circular shall also be applied to the accounts of the family members or close relatives of PEPs.
 - vi. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
 - vii. Companies offering foreign exchange offerings
 - viii. 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 centres, tax havens, countries where fraud is highly prevalent.
 - ix. Non face to face clients
 - x. Clients with dubious reputation as per public information available etc.
 - xi. Such Other persons who as per our independent judgment may be classified as CSC.
- In case we have reasons to believe that any of our existing / potential customer is a politically exposed person (PEP) we must exercise due diligence, to ascertain whether the customer is a politically exposed person (PEP), which would include seeking additional information from clients and accessing publicly available information etc.
- The dealing staff must obtain senior management`s prior approval for establishing business relationships with Politically Exposed Persons. In case an existing customer is subsequently found to be, or subsequently becomes a PEP, dealing staff must obtain senior management`s approval to continue the business relationship.
- We must take reasonable measures to verify source of funds of clients identified as PEP.

- The client should be identified by using reliable sources including documents / information and we should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
- The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in respect of statutory and regulatory requirement in future that due diligence was observed by the intermediary in compliance with the Guidelines. Each original document should be seen prior to acceptance of a copy.
- Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority.
- While accepting a client the underlying objective should be to follow the requirements enshrined in the PML Act, 2002 SEBI Act, 1992 and Regulations, directives and circulars issued there under so that we are aware of the clients on whose behalf we are dealing.

b) While carrying out transaction for the client

- RMS department of our company shall monitor the trading activity of the client and exercise due diligence to ensure that the trading activity of the client is not disproportionate to the financial status and the track record of the client.
- Payments department of our company shall ensure that payment received from the client is being received in time and through the bank account the details of which are given by the client in KYC form and the payment through cash / bearer demand drafts should not be entertained

A) Policy for acceptance of clients:

The following safeguards are followed while accepting the clients:

- a) No account is opened in a fictitious /benami name or on an anonymous basis. To ensure this we must insist the client to fill up all the necessary details in the KYC form in our presence and obtain all the necessary documentary evidence in support of the information filled in KYC. We must verify all the documents submitted in support of information filled in the KYC form with the originals and in-person verification should be done by our own staff. Moreover new client should either be introduced by an existing customer or by the senior official of the company. In case we have any doubt that in-complete / fictitious information is submitted by the client, we must ask for such additional information so as to satisfy ourselves about the genuineness of the client and the information of the client before accepting his registration. We have maintained a updated list of individuals / entities which are subject to various sanctions / measures pursuant to United Nations Security Council Resolutions (UNSCR), available from the URL <http://www.un.org/sc/committees/1267/consolist.shtml> which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc and verify the names of customers in such list of individuals and entities subject to various sanction measures of UN Security council Committee, other publicly available information and complying with Government order UAPA.
- b) Risk perception of the client need to defined having regard to:
 1. Client's location (registered office address, correspondence addresses and other addresses if applicable);
 2. Nature of business activity, trading turnover etc., and
 3. Manner of making payment for transaction undertaking.

The parameter of clients into **low, medium and high risk** should be classified. Clients of special category (as given above) may be classified as higher risk and higher degree of due diligence and regular update of KYC profile should be preformed.

Acceptance of clients through Risk – Based Approach

The clients may be higher of lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. We should apply each of the clients due diligence measures on a risk sensitive basis. Based on the client categorization, we should adopt an enhanced customer due diligence process for higher risk categories of customers. Conversely, a simplified customer due diligence process may be adopted for lower risk categories of customer. In line with the risk based approach, we should obtain type and amount of identification information and additional documents necessarily depend on the risk category of a particular customer. Further low risk provision should not apply when there are suspicious of Money laundering / financing of terrorism or when other factors give rise to a belief that the customer does not in fact pose a low risk.

- c) Ensure that no account is opened where we unable to apply appropriate clients due diligence measures / KYC policies. This shall be applicable in cases where it is not

possible to ascertain the identity of the client or information provided by the client is suspected to be non genuine or perceived non co-operation of the client in providing full and complete information. We should not continue to do business with such a person and file a suspicious activity report. *We should also evaluate whether there is suspicious trading in the account and whether there is a need to freeze or close the account.*

- d) The client account should be scrutinized regularly for determining nature of transaction taken place. *In case of any suspicious transaction arisen, the account should be frozen or securities / money should not be delivered to client.* The suspicious transaction shall be reported to the FIU as well as respective exchanges or depository where transactions have taken place.

- e) We have also evaluate whether there is suspicious trading in determining whether to freeze or close the account. Should be cautious to ensure that it does not return securities or money that may be from suspicious trades. However we can consult the relevant authorities in determining what action it should take when it suspect suspicious trading.

- f) Verify identity while carrying out:
 - Transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appears to be connected, or
 - Any international money transfer operation

Policy for Recruitment of personnel

The HR Department of our company is instructed to cross check all the references 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 References

Employees' Training

We have adopted an ongoing employee training program so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind these guidelines, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

Investors Education

Implementation of AML/CFT measures requires back office and trading staff to demand certain information from investors which may be of personal nature or which have hitherto never been

called for. Such information can include documents evidencing source of funds/income tax returns/bank records etc. This can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information. There is, therefore, a need for the back office and trading staff to sensitize their customers about these requirements as the ones emanating from AML and CFT framework. The back office and trading staff should prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the AML/CFT programme.

Procedure and manner of furnishing information.–

- (1) Every reporting entity shall communicate to the Director the name, designation and address of the Designated Director and the Principal Officer.
- (2) The Principal Officer shall furnish the information referred to in clauses (A), (B), (BA), (C), (D), (E) and (F) of sub-rule (1) of rule 3 to the Director on the basis of information available with the reporting entity. A copy of such information shall be retained by the Principal Officer for the purposes of official record.
- (3) Every reporting entity shall evolve an internal mechanism having regard to any guidelines issued by regulator, for detecting the transactions referred to in clauses (A),(B),(BA),(C),(D), (E) and (F) of sub-rule (1) of rule 3 and for furnishing information about such transactions in such form as may be directed by its Regulator.
- (4) It shall be the duty of every reporting entity, its designated director, officers and employees to observe the procedure and the manner of furnishing information as specified by its Regulator.

Procedure and manner of maintaining information. –

- (1) Every reporting entity shall maintain information in respect of transactions with its client referred to in rule 3 in accordance with the procedure and manner as may be specified by its regulator from time to time.
- (2) Every reporting entity shall evolve an internal mechanism for maintaining such information in such form and manner and at such intervals as may be specified by its regulator from time to time.
- (3) It shall be the duty of every reporting entity, its designated director, officers and employees to observe the procedure and the manner of maintaining information as specified by its regulator under subrule(1).”

Furnishing of information to the Director. –

- (1) The Principal Officer of a reporting entity shall furnish the information in respect of transactions referred to in clauses (A), (B), (BA), (C) and (E) of sub-rule (1) of rule 3

every month to the Director by the 15th day of the succeeding month.

(2) The Principal Officer of a reporting entity shall furnish the information promptly in writing or by fax or by electronic mail to the Director in respect of transactions referred to in clause (D) of sub-rule (1) of rule 3 not later than seven working days on being satisfied that the transaction is suspicious.

(3) The Principal Officer of a reporting entity shall furnish, the information in respect of transactions referred to in clause (F) of sub-rule (1) of rule 3, every quarter to the Director by the 15th day of the month succeeding the quarter.

(4) For the purpose of this rule, delay of each day in not reporting a transaction or delay of each day in rectifying a mis-reported transaction beyond the time limit as specified in this rule shall constitute a separate violation.

Customer Due Diligence

The customer due diligence (“CDD”) measures comprise the following:

- a) We obtain necessary information in order to identify persons who beneficially own or control securities account i.e. where it is appear that the securities acquired or maintained through an account are beneficially owned by a party other than the client, than party be identified via using client identification and verification procedures.
- b) Verification of customer’s identity by obtaining proper photo Identity proof i.e. passport copy, driving license copy or copy of voter id (any one of the following) and also verifying the same with originals.
- c) Verification of the beneficial ownership and control by cross checking with the details already provided by the client or by verification of details with originals.
- d) In case of corporate customers we verify the original certificate of Incorporation and Memorandum and Articles of Association and also obtain the latest Balance Sheet, Directors list of the corporate entity.
- e) 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)
- f) To verify and ask customer about his previous trading record with any other members and also directly verify with other member where the clients previously trade. Further 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.
- g) To obtain information on the purpose and intended nature of the business relationship.
- h) to determine whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner

- i) Every reporting entity shall formulate and implement a Client Due Diligence Programme, incorporating the requirements of sub-rules (1) to (13)
- j) The Client Due Diligence Programme shall include policies, controls and procedures, approved by the senior management, to enable the reporting entity to manage and mitigate the risk that have been identified either by the reporting entity or through national risk assessment.

Clients of special category (CSC):

The company consider and treated as Clients of special category on the basis of following and some other category may also come under the CSC

1. Non resident clients
2. High networth clients.
3. Trust, Charities, NGOs and organizations receiving donations
4. Companies having close family shareholdings or beneficial ownership
5. Politically exposed persons (PEP) of foreign origin
6. Current or Former Head of State, Current or Former Senior High profile politicians and connected persons including immediate family, Close advisors and companies in which such individuals have interest or significant influence
7. Companies offering foreign exchange offerings
8. Non face to face clients
9. Clients with dubious reputation as per public information available etc.

Record Keeping

1. We shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.
2. We shall 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.
3. Should there be any suspected related to 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, we shall retain the following information for the accounts of our clients 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:
 - i. the origin of the funds
 - ii. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.

- iii. the identity of the person undertaking the transaction;
 - iv. the destination of the funds;
 - v. the form of instruction and authority.
4. We shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.
5. More specifically, GCML shall put in place a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules as mentioned below:
- a) all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;
 - b) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;
 - c) 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;
 - d) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

Information to be maintained

We shall maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

- a) the nature of the transactions;
- b) the amount of the transaction and the currency in which it is denominated;
- c) the date on which the transaction was conducted; and
- d) the parties to the transaction.

Retention of Records

We have 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.

We formulate and implement the client identification program containing the requirements as

laid down in Rule 9 and such other additional requirements that it considers appropriate. The records of the identity of clients have to be maintained and preserved for a period of five years from the date of cessation of the transactions between the client and intermediary.

1. the following document retention terms should be observed:
 - (a) All necessary records on transactions, both domestic and international, be maintained at least for the minimum period.
 - (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.
2. 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 confirmed that the case has been closed.

Monitoring of transactions

1. Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money Laundering procedures.
2. We shall pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose and may specify internal threshold limits for each class of client accounts and pay special attention to the transaction which exceeds these limits. The background including all documents/office records /memorandums/clarifications sought pertaining to such transactions and purpose thereof shall also be examined carefully and findings shall be recorded in writing. Further such findings, records and related documents shall be made available to auditors and also to SEBI/stock exchanges/FIUIND/ other relevant Authorities, during audit, inspection or as and when required. These records are required to be preserved for ten years as is required under the PMLA.
3. We shall ensure a record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department.
4. Further, the compliance cell shall randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions or not.
5. All transaction alerts generated by Exchange(s) will be monitored by Principal Officer for necessary action to be taken.

Suspicious Transaction Monitoring & Reporting

1. We shall ensure that appropriate steps are taken to enable suspicious transactions to be recognised and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, we shall be guided by definition of suspicious transaction.
2. A list of circumstances which may indicate 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:
 - Clients whose identity verification seems difficult or
 - clients that appear not to cooperate
 - Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
 - Clients based in high risk jurisdictions;
 - Substantial increases in business without apparent cause;
 - Clients transferring large sums of money to or from overseas locations with instructions for payment in cash
 - Attempted transfer of investment proceeds to apparently unrelated third parties;
 - 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.
3. Any suspicious transaction shall be immediately notified to the Money Laundering Control Officer or any other designated officer within the intermediary. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall 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. The Principal Officer/Money Laundering Control Officer and other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.
4. It is likely that in some cases transactions are abandoned or aborted by clients on being asked to give some details or to provide documents. It is clarified that Company shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.
5. Clause 5.4(vii) of this Master Circular categorizes clients of high risk countries, including countries where existence and effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, as 'CSC'. Company are directed that such clients shall also be subject to appropriate counter measures. These measures may include a further enhanced scrutiny of transactions, enhanced relevant reporting mechanisms or

systematic reporting of financial transactions, and applying enhanced due diligence while expanding business relationships with the identified country or persons in that country etc.

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 Company 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.

Reporting to Financial Intelligence Unit-India

- a) In terms of the PML Rules, Company are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021.
Website: <http://fiuindia.gov.in>

- b) We shall carefully go through all the reporting requirements and formats that are available on the website of FIU – IND under the Section Obligation of Reporting Entity – Furnishing Information – Reporting Format(https://fiuindia.gov.in/files/downloads/Filing_Information.html). These documents contain detailed directives on the compilation and manner/ procedure of submission of the reports to FIU-IND. The related hardware and technical requirement for preparing reports, the related data files and data structures thereof are also detailed in these documents while detailed instructions for filing all types of reports are given in the instructions part of the related formats, we shall adhere to the following:

- a) The Suspicious Transaction Report (**STR**) shall be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his reasons for treating any transaction or a series of transactions as suspicious. It shall be ensured that there is no undue delay in arriving at such a conclusion.
 - b) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;
 - c) Utmost confidentiality shall 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.
 - d) No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.
- c) We shall not put any restrictions on operations in the accounts where an STR has been made. Company and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing (“tipping off”) the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level.

It is clarified that the registered Company, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

Risk Assessment

- a) 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 (these can be accessed at http://www.un.org/sc/committees/1267/aq_sanctios_list.shtml and <http://www.un.org/sc/committees/1988/list.shtml>).
- b) 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.

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(2) 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.

Appointment of Principal Officer

To ensure that RKSHPL properly discharge their legal obligations to report suspicious transactions to the authorities, 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 and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors. Names, designation and addresses (including e-mail addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU.

Accordingly, we have appointed Mr. Alok Kumar Jamuar as the principal officer and his appointment has been duly informed to Director-FIU.

Appointment of Designated Director

We have appointed Mr. Navdeep Varshneya as Designated Director of the Company and his appointment has been duly informed to Director-FIU. His rights and duties comprise compliance with the obligations imposed under rules and regulations.

POLICY REVIEW

Policy review has to be done in every six months by the company and last review date to be mentioned.

Last Review Done on: 15th May, 2019

