ANTI MONEY LAUNDERING POLICY

VERTEX Securities Limited

2nd floor, Thottathil Towers, Market Road, Cochin - 682 018.

Reviewed By
Mr. George Mampilly, Executive Director & CFO
on 01-11-2019

POLICY NO. 1

ANTI MONEY LAUNDERING POLICY

Vertex Securities Limited (Vertex) is committed to the highest standards of anti money laundering (AML) compliance and requires management and employees to adhere to these standards to prevent use of our products and services for money laundering purposes.

Vertex will examine its Anti Money Laundering strategies, goals and objectives on an ongoing basis and maintain an effective Anti Money Laundering program for the Company's business that reflects the best practices for a diversified, global financial services provider.

Adherence to the Company's Anti-Money Laundering Program is the responsibility of all employees. The program is formulated by the Board of Directors and directed by the Principal Officer. The program includes client screening and monitoring requirements, "know your customer" policies (including the requirement to establish the identity of beneficial owners), Embargo policies, record keeping requirements, the reporting of suspicious circumstances in accordance with relevant laws, and training.

The Background:

The Prevention Of Money -Laundering Act, 2002 (as amended) was notified on July 1, 2005. Subsequent to this, the Securities and Exchange Board of India (SEBI) has, on 18th January 2006, required market intermediaries to adopt a policy framework with respect to anti-money laundering measures to be followed by the intermediaries. Vertex is inter alia, a stock broker, depository participant and a Merchant Banker and needs to adhere to the same.

THE MONEY LAUNDERING PROCESS:

Money can be obtained illegally from various criminal activities like drug trafficking, terrorism, organized crime and fraud. As criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities and provide a legitimate cover for their source of income they usually follow three stages:

Placement

This is where the criminal proceeds are first-injected into the system. It is also the stage where those who are educated, briefed and alert to the process of money laundering, have the best chance of detecting what is happening and are thus best able to thwart and disrupt the process at the outset. At this stage, very often larger amounts of money are divided and distributed into smaller amounts to avoid suspicion and then paid into a series of bank accounts, to purchase securities, or life policies or other assets, sometimes many kinds of assets, all to achieve the prime purpose of being able to inject the tainted money or value into the legitimate mainstream financial/business system. e.g. A criminal having huge crime proceeds in form of cash, can deposit this cash in bank accounts maintained with different banks, in the name of his relatives, friends and associates, in small amounts.

Layering

After the injection has taken place and the tainted money or value has entered and become mixed up in the main mass of money or value in the financial system, it is spun around different accounts, different names, different ownerships, plus different instruments and investments. All these movements are designed to disguise the origins of the money or value and thus confuse those who might be attempting to trace the money or value back to the root, criminal source. Facilitated by the birth of electronic funds transfer technology the fast movement of funds through multiple jurisdictions often with different laws, creates major problems for investigators of identification, access and ultimately achieving successful prosecutions.

Integration

Placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as apparently legitimate funds. Integration means the reinvestment of those funds in an apparently legitimate business so that no suspicion of its origin remains and to give the appearance of legitimizing the proceeds

Definitions:

Section 3 of the Prevention of Money Laundering Act (PMLA) 2002 defines the Offence of **"Money Laundering"** as 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.

"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.

"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.

Section 4 of the Prevention of Money Laundering Act, 2002 specifies **punishment for money laundering** as under:

"4. Whoever commits the offence of money-laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extend to seven years and shall also be liable to fine which may extend to five lakh rupees.

Provided that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for the words "which may extend to seven years", the words "which may extend to ten years" had been substituted."

"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.

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.

Financial Intelligence Unit (FIU) – INDIA 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.

As per provision of section 2(n) of the Act, term "Intermediary" means: "A stock-broker, sub-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 (15 of 1992);

Objectives:

The objective is to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the Company from being used,

intentionally or unintentionally, by criminal elements". "Know Your Customer" (KYC) is the guiding principle behind the Anti-Money Laundering (AML) measures. It incorporates the "Know Your Customer" Standards & "Anti Money Laundering" Measures. KYC Standards and AML Measure, would enable the Company to know/ understand its customers the beneficial owners in case of non-individual entities, the principals behind customers who are acting as agents and their financial dealings better which in turn will help the Company to manage its risks prudently.

SEBI Mandate:

SEBI has mandated that KYC policy should be designed to combat Money Laundering which covers Customer acceptance policy and customer due diligence measures, including requirements for proper identification of the customers.

In terms of rules framed under the Act, inter alia, every intermediary shall

1. Maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place! within a month;

2. Furnish information of transactions referred to in Clause (2) to the Director within such time as may be prescribed

3. Verify and maintain the records of the identity of all its Clients, in such a manner as may be prescribed

Further in terms of rules made under the Act, all intermediaries shall maintain a record of:

1. All cash transactions of the value of **more than rupees ten lakhs** or its equivalent in foreign currency;

2. 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**;

3. All cash transaction where **forged or counterfeit currency notes** or bank notes have been used as genuine and where any forgery of a valuable security has taken place;

4. All **suspicious transactions** whether or not made in cash;

5. **Identity and current address** or addresses including permanent address or addresses of the client, the nature of business of the Client and his financial status; Provided that where it is not possible to verify the identity of the Client at the time of opening an account or executing any transaction, the Company or its authorized official shall verify the identity of the Client **within 15 days ,** after the account has been opened or the transaction has been executed.

Know Your Customer Standards:

KYC procedures enable Companies to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently. The standards set out in this Policy are minimum requirements based on applicable legal and regulatory requirements and apply for the entire Vertex Group. These requirements are intended to prevent the Company, our employees and clients from being misused for money laundering, terrorist financing or other financial crime. This Policy establishes the general framework for the fight against money laundering and financing of terrorism.

The KYC policy of the Company incorporates the following four elements:

i. Customer Acceptance Policy (CAP)

ii. Customer Identification Procedures (CIP)

iii. Risk Management; and

iv. Monitoring of Transactions

Customer (Client) Acceptance Policy (CAP)

The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in the Company. The Company shall accept customer strictly in accordance with the said policy:

i. No account shall be opened in anonymous or fictitious/benami name(s)

ii. The Company shall prepare a profile for each new customer based on risk categorization.

iii. Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc., to enable categorization of customers into low, medium and high risk called Level I, Level II and Level III respectively;

iv. The Company shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of AML Act, 2002.

v. The Company shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures i.e., branch is unable to verify the identity and/or obtain documents required as per the risk categorization due to non cooperation of the customer or non reliability of data/information furnished to the branch. The Company shall, however, ensure that these measures do not lead to the harassment of the customer. However, in case the account is required to be closed on this ground, the Company shall do so only after permission of **Principal Officer** is obtained. Further, the customer should be given a prior notice of at least 20 days wherein reasons for closure of his account should also be mentioned.

vi. The Company shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. and

vii. The Company shall continue to follow strictly the instructions regarding secrecy of customer information. The adoption of customer acceptance policy and its implementation does not become too restrictive and should not result in denial of services on listless grounds.

In brief Customer (Client) Acceptance Policy will be as follows:-

Each client should be met in person	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 filled 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 the 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.
Accept clients on whom we are able to apply appropriate KYC procedures.	All supporting documents and complete information as specified by SEBI &

	Forward Markets Commission (FMC) and 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 person 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	We should be careful while accepting and properly scrutinize the records / documents pertaining to clients belonging to below mentioned categories: a) Clients of special category like HNIs, Trust, Charities, NGOs, Politically Exposed Persons (PEP) persons of foreign origin; b) 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. c) Current/Former Head of State, Current/Former Senior high profile politician, Companies offering foreign exchange, etc. d) Clients from high-risk countries viz. Libya, Pakistan, Afghanistan, etc. or clients belonging to countries where corruption/fraud level is high viz. 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 Mandatory information / documents and Financial Details	Clients 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 refuses to provide information/documents and we should have sufficient reason and record to reject the client ‘s request towards reluctance. Client ‘s account should be opened only on receipt of financial details along with supporting documents, viz. ITR, Copy of Annual Accounts, Copy of Form 16 in case of salaried employees signed by CA, Bank Account Statement for fast 6 months. Self declaration along with relevant documents.

Customer Identification Procedure (CIP)

Customer identification means identifying the person and verifying his/her identity by using reliable, independent source documents, data or information.

The branches need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer. Being satisfied means that the branch is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance of the guidelines in place.

Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate, etc).

For customers that are natural persons, the branches shall obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph.

For customers that are legal persons or entities, the branches shall (i) verify the legal status of the legal person/entity through proper and relevant documents (ii) verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of that person (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

Customer Identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given below for the guidance of branches If the branch decides to accept such accounts in terms of the Customer Acceptance Policy, the branch shall take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are.

<u>An indicative list of the nature and type of documents/information that may be relied upon for customer identification is</u>

In case of individuals, one copy of the following documents have to be obtained.	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 identify are Voter's Identity Card, Passport, Ration Card or any Government /PSU Bank issued photo identify 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.
In case of Corporates, one certified copy of the following documents must be obtained.	Copy of the Registration / Incorporation Certificate Copy of the Memorandum & Articles of Association, Copy of the PAN Card and Director Identification No. (DIN). Copy of Net-worth Certificate Latest Income Tax Return filed. Board Resolution for appointment of the

	Authorized Person(s) who will operate the account. Proof of address and identify of Authorized Person(s).
In case of a Trust, one certified copy of the following must be obtained	Registration Certificate Trust Deed PAN Card Authorization letter for the entity authorized to act on their behalf. Officially valid documents viz. PAN Card, Voter's ID, Passport, etc. of person(s) authorized to transact on behalf of the Trust.

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 about 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. Business Head should be alerted, client be contacted immediately on telephone and the trading, if suspected, should be suspended. If Employee of Vertex introduces the client, exact relation of the client with such employee should be documented.
6. For scrutiny / background check of the Franchisee, websites such as www.watchoutinvestors.com should be referred. Also, Prosecution Database / List of Vanishing Companies available on www.fmc.gov.in; www.mcxindia.com; www.ncdex.com; www.nmce.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 or traceable or contract 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 Regional Business Head. The Regional Business Head will, in turn, discuss the same with the Principal Officer to decide on the necessary course of action, including reporting to FIU, New Delhi

Risk Management:

The risk level of the customer shall be assigned on the following basis:

i. Low Risk (Level I):

Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk.

The 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 whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases, only the basic requirements of verifying the identity and location of the customer shall be met.

ii. Medium Risk (Level II):

Customers those are likely to pose a higher than average risk to the Company may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

a) Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading / business activity.

b) Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious.

iii. High Risk (Level III):

The branches may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom the sources of funds are not clear. The examples of customers requiring higher due diligence may include:

a) Non Resident Customers,

b) High Net worth individuals

c) Trusts, charities, NGOs and organizations receiving donations,

d) Companies having close family shareholding or beneficial ownership

e) Firms with 'sleeping partners'

f) Politically Exposed Persons (PEPs) of foreign origin

g) Non-face to face customers, and

h) Those with dubious reputation as per public information available, etc.

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.

Risk Assessment:

Risk assessment shall be carried out 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_sanctions_list.shtml and http://www.un.org/sc/committees/1988/list.shtml).

The risk assessment shall be carried out by branches considering 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.

Clients should provide KYC details within 2 years for High Risk category, 4 years for Medium Risk category and 6 years for Low Risk category.

KYC reconfirmation:

The KYC reconfirmation request received by NSDL is reconfirmed through the details provided in I-Assist . After confirmation of the data the details will be submitted in I-Assist.

Monitoring Transactions:

Continuous monitoring is an essential ingredient of effective KYC procedures and the extent of monitoring should be according to the risk sensitivity of the account.

Branches shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. High risk accounts shall be subjected to intensive monitoring

suspicious transactions involve funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under the law; The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the Company knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Criteria in relation to defining suspicious transaction:

It is difficult to define exactly what constitutes suspicious transactions and as such given below is a list of circumstances where transactions may be considered to be suspicious in nature. This list is only inclusive and not exhaustive. Whether a particular transaction is actually suspicious or not will depend on the background, details of the transactions and other facts and circumstances.

1. Complex /unusually large transactions/ patterns which appear to have no economic purpose.
2. Client having suspicious background or links with known criminals
3. Clients whose identity verification seems difficult.

For Example:

i. False identification documents
ii. Identification documents which could not be verified within reasonable time
iii. Non face to face Client
iv. Doubt over the real beneficiary of the account
v. Accounts opened with names very close to other established business entities.

4. Client appears not to co-operate.

5. Use of different accounts by Client alternatively.

6. Sudden activity in dormant accounts

7. Multiple accounts
    i. Large number of account having a common account holder, authorized signatory with no rationale
    ii. Unexplained transfers between multiple accounts with no rationale
8. Asset management services for clients where the sources of funds is not clear or not in keeping with the clients' apparent standing/business activity.

9. Substantial increase in business without apparent cause (Unusual activity compared to past transactions)

10. Activity materially inconsistent with what would be expected from declared business.

11. Inconsistency with clients apparent financial standing.

12. Unusual transactions by Clients of Special Category (CSCs) and business undertaken by shell corporations, offshore banks/financial services, businesses reported to be in the nature of export-import of small items.

13. A transaction which gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime.

14. A transaction which appears to be a case of insider trading

15. Transactions reflect likely market manipulations

16. Suspicious off market transactions

17. Value of transaction just under the reporting threshold amount in an apparent attempt to avoid reporting or Multiple transactions of value just below the threshold limit specified in PMLA so as to avoid possible reporting;

18. Inconsistency in the payment pattern by the client

19. Trading activity in account of high risk clients based on their profile, business pattern and industry segment.

20. Accounts based as 'passed through'. Where no transfer of ownership of securities or trading is occurred in the account and the account is being used only for layering purposes.

21. Large deals at prices away from the market

22. Purchases made in one client's account and later on transferred to a third party through off market transactions through DP Accounts.

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:

Report	Description	Due Date
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, Zonal Business Heads are required to collect information from the Branches/Departments/Sub-brokers under their control/ jurisdiction and submit report on Cash transactions on monthly basis, to **Principle Officer** by the 10th day of the following month and suspicious transactions to the Principle Officer 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 of 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.

Record Keeping*:*

The Company Shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made hereunder, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

Company 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.

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, Company shall retain the following information for the accounts of their customers 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, the origin of the funds, the form in which the funds were collected or withdrawn, e.g. cash, cheques, etc. the identity of the person undertaking the transaction, the destination of the funds, the form of instruction and authority.

The Company shall ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, Company shall consider retaining certain records, 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.

Retention of Records:

The following document retention terms shall be observed:

(a) All necessary records on transactions shall be maintained at least for the minimum period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.

(b) 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 shall also be kept for the same period as stated above..

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

Designated Principal Officer:

In case any further information /clarification are required in this regard, the Principal Officer may be contacted:

Mr. George Mampilly [Designation: Executive Director& CFO]

Address: Thottathil Towers,
2nd Floor, Market Road
Kochi, Kerala – 682 018
Office No: 91-484-2384848
Mobile: +91-9387326826
Email Id: mampilly@vertexbroking.com

Appointment of a Designated Director:

In addition to the existing requirement of designation of a Principal Officer, we have appointed a "Designated Director" under the purview of Rule 2 (ba) of the PML Rules. The detail of Designated Director is given below:

Name: Mr. U. Ramachandran [Designation: Managing Director]

Address: **Vertex Securities Ltd**
2ND Floor, Thottathil Towers,
Market Road
Kochi, Kerala – 682 018
Office No.:0484-2384848
Email ID: ramachandran_u@hotmail.com

To,
The Principal Officer,
Vertex Securities Limited.

Undertaking

I hereby undertake that, I _____ shall abide by the requirements under Prevention of Money Laundering Act, 2002 (PMLA) and Anti Money Laundering Policy of Vertex Securities Limited as approved by the Board of Directors of the Company.

Date:
Place: Signature: