PMLA POLICY

Version: 2023.01

Approved by Board on July 28, 2023

Introduction of Exatrade Technologies is a member of National Stock Exchange of India Limited & BSE Limited, having SEBI Regn No. INZ000309029.

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 February 03, 2023 and rules laid down by FIU.

Section 1: Overview

1.1 Introduction and Background of AML

SEBI has issued necessary directives vide circulars from time to time, covering issues related to Know Your Client (KYC) norms, Anti-Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing of Terrorism (CFT).The Prevention of Money Laundering Act, 2002 (PMLA) has been brought into force with effect from 1st July 2005 by the Department of Revenue, Ministry of Finance, and Government of India.

The Directives given by SEBI are intended for the use primarily by intermediaries registered under Section 12 of the SEBI act 1992. The overriding principle is that the intermediaries should be able to satisfy themselves that the measures taken by them are adequate, appropriate and abide by the spirit of such measures and the requirements as enshrined in the PMLA .The PMLA has been further amended vide notification dated March 06,2009 and inter-alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as prescribed in Section 12 A read with Section 24 of the SEBI Act 1992 will now be treated as a scheduled offence under Schedule B of PMLA.

On February 03, 2023 a master circular no SEBI/HO/MIRSD/MIRSD-SEC- 5/P/CIR/2023/022 consolidating all the requirements/ instructions has been issued by SEBI which supersedes all the earlier circulars. As per the provisions of PMLA and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (Maintenance of Records Rules), as amended from time to time and notified by the Government of India, every reporting entity (which includes intermediaries registered under section 12 of the SEBI Act, i.e. a stock-broker, share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, asset management company, depository participant, merchant banker, portfolio manager, investment adviser and any other intermediary associated with the securities market and registered under Section 12 of the SEBI Act and stock exchanges), shall have to adhere to the client account opening procedures, maintenance records and reporting of such transactions as prescribed by the PMLA and rules notified there under.

1.2 Policies and procedures to combat Money Laundering and Terrorist Financing

1.2.1 Obligation to establish policies and procedures: -

a) Global measures taken to combat drug trafficking, terrorism and other

organized and serious crimes have all emphasized the need for financial institutions, including securities market intermediaries, to establish internal procedures that effectively serve to prevent and impede money laundering and terrorist financing. The PMLA is in line with these measures and mandates that all intermediaries ensure the fulfillment of the aforementioned obligations.

b) To be in compliance with these obligations, the senior management of a registered intermediary shall be fully committed to establishing appropriate policies and procedures for the prevention of ML and TF and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements. The Registered Intermediaries shall :-

i) issue a statement of policies and procedures, where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements;
ii) ensure that the content of these Directives are understood by all staff members ;
iii) regularly review the policies and procedure to ensure their effectiveness ;
iv) adopt client acceptance policies and procedures
v) undertake client due diligence (CDD) measures to an extent that is sensitive to the risk of ML and TF depending on the type of client , business relationship or transaction;
vi) have system in place for identifying , monitoring and reporting suspected ML or TF transactions to the law enforcement authorities
vii) develop staff members awareness and vigilance to guard against ML and TF;

1.2.2 Policies and procedures to combat ML shall cover:-

a) Communication of company policies relating to prevention of ML and TF to all management and relevant staff;
b) Client acceptance policy and client due diligence measures;
c) Maintenance of records;
d) Compliance with relevant statutory and regulatory requirements;
e) Co-operation with the relevant law enforcement authorities including timely disclosure of information;
f) Role of internal audit or compliance function to ensure compliance with the policies, procedures and controls relating to the prevention of ML and TF. The Internal audit function shall be independent, adequately resourced and commensurate with the size of the business and operations, organization structure and number of clients and other such factors.

Section 2: Detailed Directives

2.1 Vision towards Anti Money Laundering

2.1.1 Exatrade Technologies 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.

2.1.2 EXATRADE TECHNOLOGIES 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 ranging Rs.500 to Rs.1000. Hence the requirement of maintaining record of cash transaction in excess of Rs.10 Lakh is ruled out.

2.1.3 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 behavior etc.

2.1.4 Compliance department of EXATRADE TECHNOLOGIES review & update PMLA policy on time to time based on the circular issued by regulator in consultation with Principal Officer.

2.2 Client Due Diligence (CDD)

2.2.1 The CDD measures comprise the following:

(a) Obtaining sufficient information in order to identify person who beneficially own or control the 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 are 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.

(b) Verify the client‟s identity using reliable, independent source documents, data or information;

(c) Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted-

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

aa) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to:

i. more than 10% of shares or capital or profits of the juridical person, where the juridical person is a company;

ii. more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or

iii. more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

bb) In cases where there exists doubt under clause (aa) above as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner.

cc) Where no natural person is identified under clauses (aa) or (bb) above, the identity of the relevant natural person who holds the position of senior managing official.

ii. **For client which is a trust:** Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the

protector, the beneficiaries with 10% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

Where the client is a non-profit organisation, the intermediary shall register the details of a client, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the registered intermediary has ended or the account has been closed, whichever is later.

iii. **Exemption in case of listed companies:** Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

iv. **Applicability for foreign investors:** Intermediaries dealing with foreign investors" may be guided by the clarifications issued vide SEBI circulars CIR/MIRSD/11/2012 dated September 5, 2012 and CIR/ MIRSD/ 07/ 2013 dated September 12, 2013, for the purpose of identification of beneficial ownership of the client.

v. The compliance of the aforementioned provision on identification of beneficial ownership shall be monitored by Board of Directors of EXATRADE TECHNOLOGIES.

(d) Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c)

(e) Understand the ownership and control structure of the client;

(f) 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 Exatrade Technologies knowledge of the client, its business and risk profile, taking into account, where necessary,the client"s source of funds; and

(g) We shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.

2.2.2 Policy for acceptance of clients:

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

b) Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients‟ location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters shall enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary,be classified even higher. Such clients require higher degree of due diligence and regular update of Know Your Client (KYC) profile.

c) Do not accept clients with identity matching persons known to have criminal background: - We take undertaking from the client whether they have criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings or by any enforcement/regulatory agency worldwide. If yes, we do not open the client account.

d) **Each client should be met in person:** We have to perform the in person verification process very diligently. Either the client should visit the company/business associates office or concerned official/business associates may visit the client at their residence / office address. Official /Business associates also verify photocopy of the documents with the original. As far as possible, try to open account of known person or person introduce by an existing client. Further, we also capture the introducer detail in account opening form.

e) Accept clients on whom we are able to apply appropriate KYC procedures: Obtain complete identification information from the client. It should be ensured that the initial forms taken by the client are filled in completely. All photocopies submitted by the client should be checked against original documents without any exception. 'Know Your Client' guidelines should be followed without any exception. All supporting documents as specified by Securities and Exchange Board of India (SEBI) and Exchanges should be obtained and verified.

f) Be careful while accepting Clients of Special category: We should be careful while accepting clients of special category like (1) NRIs (2) HNIs- Client having networth of Rs. 25 crore or more (3) Trust, Charities, NGOs (4) Politically Exposed Persons (PEP) (5) companies having closed share holding/ beneficial ownership (6) Companies dealing in/offering foreign currency (7) Clients in high risk countries (like Libya, Pakistan, Afghanistan, etc.) (8) Non face to face clients (9) Clients with dubious background. Clients belonging to countries where corruption/fraud level is high (like Nigeria, Burma, etc). Scrutinize

minutely the records/ documents pertaining to clients belonging to aforesaid category. We also define the category of client in back office software.

g) **Do not compromise on submission of mandatory information/ documents:** Client's account should be opened only on receipt of mandatory information along with authentic supporting documents as per the regulatory guidelines. Accounts where the client refuses to provide information/documents should not be opened. We shall capture data of key person like director & shareholder of all non-individual clients & also taking complete details/documents of Director/ Trustee/ Partners etc mandatory while opening the account. In case of corporate client in order to identify client with cross holding, we capture key person data like details of director, share holder.

h) Verify and Validate circumstances under which the client is permitted to act on behalf of another person/ entity are clearly laid down. It is specified in what manner the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/ value and other appropriate details. Further the rights and responsibilities of both the persons (i.e. the agent- client registered with EXATRADE TECHNOLOGIES, as well as the person on whose behalf the agent is acting is clearly laid down). Adequate verification of a person‟s authority to act on behalf the client is also carried out.

i) The CDD process shall necessarily be revisited, if required, when there are suspicions of money laundering or financing of terrorism (ML/FT).

2.2.3 Risk-based Approach:

2.2.3.1 It is generally recognized that certain clients may be of a higher, medium or lower risk category depending on the circumstances such as the client's financial background, type of business relationship or transaction etc. As such shall apply each of the clients due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that we shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for other risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that registered intermediaries shall obtain necessarily depend on the risk category of a particular client.

2.2.3.2 Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

2.2.3.3 Risk Assessment

a) We shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to our 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 the URL - http://www.un.org/sc/committees/1267/aq_sanctions_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.

2.2.3.4 Risk Classification

We should accept the clients based on the risk they are likely to pose. The aim is to identify clients who are likely to pose a higher than average risk of money laundering or terrorist financing. For this purpose, we need to classify the clients as low risk, medium risk and high risk clients. By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high risk client we have to apply higher degree of due diligence.

Special attention must be paid to the transactions which are complex, unusually large or pattern which appears to have no economic purpose. Risk profiling is to divide into two broad categories one is on-board risk & second is ongoing risk. On-bard risk is defined when a client is introduced to the company.

Risk categorization of client will be based on following parameters:

a) If the client‟s location (registered office address, correspondence address) is out of India and in any of the high risk jurisdictions as defined by FATF.
b) Individual Client having annual income more than Rs. 1 Crores and/or Networth of Rs. 25 Crores.
c) Income & Networth does not commensurate with transactions (Trading/ DP).
d) Client dealing in Forex.

Category will be assigned based on the following criteria:

a) High - Meets all four parameters.
b) Medium - Meets three parameters
c) Low - Meets two or less

Special category customers & clients reported to FIU shall also move to the high risk category.

2.2.4 Client of special category (CSC): Such clients shall include the following:

a) Non - resident clients
b) High net-worth clients,
c) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations
d) Companies having close family shareholdings or beneficial ownership
e) 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.
f) Companies offering foreign exchange offerings
g) 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 centers, tax havens, countries where fraud is highly prevalent. While dealing with

clients in high risk countries where the existence/effectiveness of money laundering control is suspect, intermediaries apart from being guided by the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), shall also independently access and consider other publicly available information.

h) Non face to face clients

i) Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and EXATRADE TECHNOLOGIES shall exercise independentjudgment to ascertain whether any other set of clients shall be classified as CSC or not.

2.2.5 Client identification procedure:

2.2.5.1 Requirements of a Client Identification Procedure (CIP):

a) We shall proactively put in place appropriate risk management systems to determine whether our 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. Further, the enhanced CDD measures as outlined in clause 2.2.5 shall also be applicable where the beneficial owner of a client is PEP.

b) We shall obtain approval from Principal Officer/ Designated Director 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, Principal Officer/ Designated Director‟s approval is mandatory to continue the business relationship.

c) We 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 using reliable sources including documents/ information. We 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 EXATRADE TECHNOLOGIES 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 (Principal Officer).

2.2.5.2 SEBI has prescribed the minimum requirements relating to KYC for certain classes of registered intermediaries from time to time. EXATRADE TECHNOLOGIES shall frame its own internal directives based on its experience in dealing with its clients and legal requirements as per the established practices.

Further, the EXATRADE TECHNOLOGIES shall conduct ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued there under so that the intermediary is aware of the clients on whose behalf it is dealing.

2.2.5.3 EXATRADE TECHNOLOGIES shall formulate and implement a CIP which shall incorporate the requirements of the PML Rules Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of recordsof the identity of the clients and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

2.2.5.4 It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to EXATRADE TECHNOLOGIES from obtaining the minimum information/ documents from clients as stipulated in the PML Rules/ SEBI Circulars (as amended from time to time) regarding the verification of the records of the identity of clients. Further no exemption from carrying out CDD exists in respect of any category of clients. In other words, there shall be no minimum investment threshold/ category-wise exemption available for carrying out CDD measures by registered intermediaries. This shall be strictly implemented by all intermediaries and non-compliance shall attract appropriate sanctions.

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

2.2.6.1 We 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.

2.2.6.2 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 we shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

2.3 Record Keeping

2.3.1 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.

2.3.2 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.

2.3.3 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.

2.3.4 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.

2.3.5 More specifically, EXATRADE TECHNOLOGIES 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.

2.4.1 Information to be maintained

2.4.1 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.

2.5 Retention of Records

2.5.1 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. Further, the records

mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions between the client and EXATRADE TECHNOLOGIES.

2.5.2 As stated in sub-section 2.2.5, we implement the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of 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 has ended or the account has been closed, whichever is later.

2.5.3 Thus the following document retention terms shall be observed:

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

b) We shall maintain and preserve the records of documents evidencing the identity of its clients and beneficial owners (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence for a period of five years after the business relationship has ended or the account has been closed, whichever is later.

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

2.5.5 **Records of information reported to the Director, Financial Intelligence Unit – India (FIU – IND)**: We shall maintain and preserve the records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, for a period of five years from the date of the transaction.

2.6 Monitoring of transactions

2.6.1 Regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if we have an understanding of the normal activity of the client so that it can identify deviations in transactions/ activities.

2.6.2 We shall pay special attention to all complex unusually large transactions/ patterns which appear to have no economic purpose. We may specify internal threshold limits for each class of client accounts and pay special attention to

transactions 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 maintained and preserved for a period of five years from the date of transaction between the client and EXATRADE TECHNOLOGIES.

2.6.3 We shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transaction of a suspicious nature or any other transactions notified under Section 12 of the Act are reported to the Director, FIU-IND. Suspicious transactions shall also be regularly reported to the Principal Officer/ Designated Director.

2.6.4 Further, the compliance cell shall randomly examine a selection of transactions undertaken by clients to comment on their nature i.e. whether they are in the nature of suspicious transactions or not.

2.6.5 All transaction alerts generated by Exchange(s) will be monitored by Principal Officer for necessary action to be taken.

2.7 Suspicious Transaction Monitoring and Reporting

2.7.1 We shall ensure that appropriate steps are taken to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. While determining suspicious transactions, we shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

2.7.2 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 that appear 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 based in high risk jurisdictions;
d) Substantial increases in business without apparent cause;
e) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;

f) Attempted transfer of investment proceeds to apparently unrelated third parties;
g) 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.

2.7.3 Any suspicious transaction shall be immediately notified to the Principal Officer. 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 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.

2.7.4 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 we shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

2.7.5 Clause 2.2.4 (g) of this policy 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". 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.

2.8 List of Designated Individuals/ Entities

An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at **http://www.un.org/sc/committees/1267/consolist.shtml**. EXATRADE TECHNOLOGIES shall ensure thataccounts are not opened in the name of anyone whose name appears in said list. EXATRADE TECHNOLOGIES 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.

2.9 Procedure of freezing of funds, financial assets or economic resources or related services

2.9.1 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.

2.9.2 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.

2.9.3 We shall ensure effective and expeditious implementation of the procedure laid down in the UAPA Order dated August 27, 2009 as listed below:

a) On receipt of the updated list of individuals/ entities subject to UN sanction measures (hereinafter referred to as 'list of designated individuals/ entities) from the Ministry of External Affairs (MHA) and forwarded by SEBI. EXATRADE TECHNOLOGIES shall take following steps:

i. Shall maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of securities with them.

ii. In the event, particulars of any of customer/s match the particulars of designated individuals/entities, EXATRADE TECHNOLOGIES shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer on our books to the Joint Secretary (IS.I), Ministry of Home Affairs,

at Fax No.011-23092569 and also convey over telephone on 011- 23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in.

iii. We shall send the particulars of the communication mentioned in (ii) above through post/fax and through e-mail (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051 as well as the UAPA nodal officer of the state/UT where the account is held, as the case may be, and to FIU-IND.

iv. In case the aforementioned details of any of the customers match the particulars of designated individuals/entities beyond doubt, stock exchanges, depositories and registered intermediaries would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed through e-mail at jsis@nic.in.

v. EXATRADE TECHNOLOGIES shall also file a Suspicious Transaction Report (STR) with FIU- IND covering all transactions in the accounts covered by paragraph
2.9.2 (a) (ii) above carried through or attempted, as per the prescribed format.

b) On receipt of the particulars as mentioned in paragraph 2.9.3 (a) (ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and /or the Central Agencies so as to ensure that the individuals/ entities identified by EXATRADE TECHNOLOGIES are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by EXATRADE TECHNOLOGIES are held by the designated individuals/entities. This verification would be completedwithin a period not exceeding 5 working days from the date of receipt of such particulars.

c) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned depository under intimation to SEBI and FIU-IND. The

order shall take place without prior notice to the designated individuals/entities.

d) Implementation of requests received from foreign countries under U.N. Securities Council Resolution 1373 of 2001.

i. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.

ii. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

iii. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officer in SEBI. The proposed designee, as mentioned above would be treated as designated individuals/entities.

iv. Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to EXATRADE TECHNOLOGIES and the procedure as enumerated at paragraphs 2.9.2 (a) and (b) shall be followed.

v. The freezing orders shall take place without prior notice to the designated persons involved.

e) Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

i. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, shall move an application giving the requisite evidence, in writing, to EXATRADE TECHNOLOGIES. EXATRADE TECHNOLOGIES shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 5(ii) above within two working days. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned stock exchanges, depositories and EXATRADE TECHNOLOGIES. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

f) Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

i. All Orders under section 51A of the UAPA relating to funds, financial assets or economic resources or related services, would be communicated to stock exchanges, depositories and EXATRADE TECHNOLOGIES through SEBI.

2.10 Reporting to Financial Intelligence Unit-India

2.10.1 In terms of the PML Rules, we are required to report information relating to 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

2.10.2 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 STR to FIU-IND;
c) Utmost confidentiality shall be maintained in filing of STR to FIU-IND.
d) No nil reporting needs to be made to FIU-IND in case there are no suspicious transactions to be reported.

2.10.3 We shall not put any restrictions on operations in the accounts where an STR has been made. Our 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 intermediaries, 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.

2.11 Appointment of Principal Officer

To ensure that EXATRADE TECHNOLOGIES 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. Hari Shankar Gupta as the principal officer & Designated Partner and his appointment has been duly informed to Director-FIU.

2.12 Appointment of Designated Director

We have appointed Mr. Hari Shankar Gupta as Designated Partner of the firm and his appointment has been duly informed to Director-FIU. His rights and duties comprise compliance with the obligations imposed under rules and regulations.

2.13 Guidelines for Employees Hiring/ Employees Training/Investor Education

We have adequate screening procedures in place to ensure high standards while hiring employees. We have regular training programmes, where the staff members (front office, back office, compliance, risk etc) are updated about the AML and CFT procedures. To implement AML/ CFT measures, at times we may be required to collect documents like source of funds/ income tax return/bank records from the client who may arise questioning by the client. To address these queries we must sensitize and educate our clients about these requirements. We also inform our business associates/branch about the AML policy.