

COMPOSITE INVESTMENTS PRIVATE LIMITED
POLICIES AND PROCEDURE
FOR COMBATING MONEY LAUNDERING (ML) OR TERRORIST FINANCING (TF)
(Adopted as per the requirements of the PMLA Act)

Applicability

Composite Investments Private Limited (CIPL), is a SEBI Registered Intermediary (Broking/ DP/Portfolio Manager)

In compliance with

- The PMLA Act 2005 as amended from time to time and rules thereof
- SEBI Circular and Directives including SEBI Master Circular ref. SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated 06-June-2024.

1. CIPL Policy

It is our policy to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

2. Anti Money Laundering Policy:

2.1. Written Anti Money Laundering Procedures

CIPL has adopted these written procedures to implement the anti- money laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia, the following three specific parameters which are related to the overall 'Client Due Diligence Process':

- a) Policy for acceptance of clients
- b) Procedure for identifying the clients
- c) Risk Management
- d) Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR).

2.2. Client Due Diligence (CDD)

2.2.1 The CDD measures at CIPL shall comprise the following:

- a) Obtaining sufficient information in order to identify persons 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 shall be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement
- b) Verify the client's identity using reliable, independent source documents, data or information. Where the client purports to act on behalf of juridical person or individual or trust, CIPL shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.
- c) Identifying 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, CIPL 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, CIPL shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the author 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.

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 will not be necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

iv. Applicability for foreign investors

While dealing with foreign investors, CIPL will be guided by the SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client.

v. Monitor of compliance

The compliance of the aforementioned provision on identification of beneficial ownership shall be monitored by the Compliance officer/Director of CIPL

d) Verifying 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) Understanding the ownership and control structure of the client.

f) Conducting 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 CIPL's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds

g) CIPL shall review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship, as the case may be, when there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained client identification data; and

h) CIPL shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process

i) CIPL shall register the details of a client, in case of client being a non-profit organisation, 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

j) Where CIPL is suspicious that transactions relate to money laundering or terrorist financing, and reasonably believes that performing the CDD process will tip-off the client, the registered intermediary shall not pursue the CDD process, and shall instead file a STR with FIU-IND

2.2.2 Policy for acceptance of clients:

2.2.2.1 The client acceptance policies and procedures of CIPL is a part of the "CIPL Client On boarding and Periodical Review Policy" (Attached as Annexure A) and aims to identify the types of clients that are likely to pose a higher than average risk of ML or TF. By establishing such policies and procedures, CIPL will be in a better position to apply client due diligence on a risk sensitive basis depending on the type of client business relationship or transaction. In a nutshell, the following safeguards will be followed while accepting the 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) CIPL shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC). CSC shall include the following:

i) Non - resident clients;

ii) High net-worth clients;

iii) Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations

iv) Companies having close family shareholdings or beneficial ownership

v) Politically Exposed Persons (PEP). PEP shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. The additional norms applicable to PEP as contained in paragraph 14 of the SEBI Master Circular shall also be applied to the accounts of the family members or close relatives of PEPs

vi) Clients in high risk countries.

While dealing with clients from or situate in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspect, CIPL, apart from being

guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org) from time to time, shall also independently access and consider other publicly available information along with any other information which CIPL may have access to

vii) Non face to face clients.

Non face to face clients means clients who open accounts without visiting the branch/offices of CIPL or meeting the officials of CIPL. Video based customer identification process shall be carried which is treated as face-to-face onboarding of clients;

viii) Clients with dubious reputation as per public information available

d) Documentation requirements and other information to be collected in respect of different classes of clients depending on the perceived risk and having regard to the requirements of Rule 9 of the PML Rules, Directives and Circulars issued by SEBI from time to time.

e) Ensure that an account is not opened where CIPL is unable to apply appropriate CDD measures/ KYC policies. This shall apply in cases where it is not possible to ascertain the identity of the client, or the information provided to CIPL is suspected to be non - genuine, or there is perceived non - co-operation of the client in providing full and complete information. CIPL shall not continue to do business with such a person . It shall also evaluate whether there is suspicious trading in determining whether to freeze or close the account. CIPL shall be cautious to ensure that we do not return securities of money that may be from suspicious trades. However, CIPL shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

f) The circumstances under which the client is permitted to act on behalf of another person / entity shall be clearly laid down. It shall be specified in what manner the account shall 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 CIPL, as well as the person on whose behalf the agent is acting shall be clearly laid down. Adequate verification of a person's authority to act on behalf of the client shall also be carried out.

g) Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match 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 agency worldwide

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

2.2.3 Client identification procedure:

2.2.3.1 The KYC policy shall clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the client relationship, while carrying out transactions for the client or when CIPL has doubts regarding the veracity or the adequacy of previously obtained client identification data. CIPL shall be in compliance with the following requirements while putting in place a Client Identification Procedure (CIP):

a) CIPL shall proactively put in place appropriate risk management systems to determine whether its existing client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs..

- b) Senior management approval would be obtained 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, CIPL shall obtain approval from Director to continue the business relationship.
- c) CIPL 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 CIPL by using reliable sources including documents / information. CIPL 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 CIPL 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)

2.2.3.2 SEBI has specified the minimum requirements relating to KYC from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been specified or which may be specified by SEBI from time to time, CIPL shall frame their own internal directives based on their experience in dealing with their clients and legal requirements as per the established practices. Further, CIPL 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 thereunder so that the CIPL is aware of the clients on whose behalf it is dealing.

2.2.3.3 CIPL 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 records of the identity of the clients and such other additional requirements that is considered appropriate to enable CIPL to determine the true identity of its clients.

2.2.3.4 It may be noted that irrespective of the amount of investment made by clients, no minimum threshold or exemption is available to CIPL 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 CIPL. This shall be strictly implemented by CIPL.

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

2.2.4.1 CIPL 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.

2.2.4.2 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. In this regard, CIPL shall:

- i) CIPL shall immediately obtain necessary information of such client due diligence carried out by the third party

- ii) CIPL shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
- iii) CIPL shall be satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act
- iv) The third party is not based in a country or jurisdiction assessed as high risk

Further, it is clarified that CIPL shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable

2.3 Risk Management:

2.3.1 -Risk Based Approach:

2.3.1.1: CIPL shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and should have policies approved by their senior management, controls and procedures in this regard. Further, CIPL shall monitor the implementation of the controls and enhance them if necessary

2.3.1.2: It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, CIPL shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that CIPL 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 lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that CIPL shall obtain necessarily depend on the risk category of a particular client. 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

2.3.2 – Risk Assessment:

2.3.2.1 : CIPL 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

2.3.2.2 : 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

CIPL shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. CIPL shall ensure:

- a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and
- b. Adoption of a risk based approach to manage and mitigate the risks

2.3.2.3: 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

2.4 Monitoring of Transactions:

2.4.1: CIPL understands that regular monitoring of transactions is vital for ensuring effectiveness of the AML procedures. This is possible only if CIPL has an understanding of the normal activity of the client so that it can identify deviations in transactions / activities

2.4.2: CIPL shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. CIPL 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/FIU-IND/ other relevant Authorities, during audit, inspection or as and when required

2.4.3: CIPL shall apply client due diligence measures also to existing clients on the basis of materiality and risk, and conduct due diligence on such existing relationships appropriately. The extent of monitoring shall be aligned with the risk category of the client

2.4.4 : CIPL shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions 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 higher authorities within the intermediary

2.4.5: Further, the compliance cell of CIPL 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.

2.5. Record Keeping

2.5.1 CIPL 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.

2.5.2 CIPL 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 behaviour.

2.5.3 Should there be any suspected 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, CIPL shall retain the following information for the accounts of their 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.

2.5.4 CIPL 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, CIPL 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.

2.5.5 More specifically, CIPL 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. For the purpose of suspicious transactions reporting, apart from ‘transactions integrally connected’, ‘transactions remotely connected or related’ shall also be considered
- 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 including, inter-alia, credits or debits into or from any non-monetary account such as demat account, security account maintained by CIPL.

2.6. Information to be maintained

2.6.1 CIPL will 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.

2.7. Retention of Records

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

2.7.2 As stated in sub-section 2.2.3, CIPL is required to formulate and implement the CIP containing the requirements as laid down in Rule 9 of the PML Rules and such other additional requirements that it considers appropriate. Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of eight years after the business relationship between the clients and CIPL has ended or the account has been closed, whichever is later.

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

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

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

2.8. Monitoring of transactions

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

2.8.2 CIPL shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose. CIPL 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 will be maintained and preserved for a period of eight years from the date of transaction between the clients and CIPL.

2.8.3 CIPL shall ensure a record of the transactions is preserved and maintained in terms of Section 12 of the PMLA and that transactions 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 higher authorities (Director) within CIPL.

2.8.4 Further, the compliance cell of CIPL 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.

2.8.5 All regulatory alerts generated by the Market Infrastructure Institutions (MIIs) shall be monitored by the Principal Officer for necessary action to be taken

2.9. Suspicious Transaction Monitoring and Reporting

2.9.1 CIPL 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, CIPL shall be guided by the definition of a suspicious transaction contained in PML Rules as amended from time to time.

2.9.2 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.

2.9.3 Any suspicious transaction shall be immediately notified to the Money Laundering Control Officer (Principal Officer) or any other designated officer within CIPL. 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.

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

2.9.5 Clause 2.2.2.1 c (vi) 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.

2.10. List of Designated Individuals/ Entities

2.10.1 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>. CIPL shall ensure that accounts are not opened in the name of anyone whose name appears in said list. CIPL 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.

2.11. Procedure for freezing of funds, financial assets or economic resources or related services

2.11.1 In terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they do not have any accounts in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC).

2.11.2 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.

2.11.3 CIPL 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, CIPL shall take the followings steps:

i. CIPL will 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. CIPL shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements

ii. In the event, particulars of any of customer/s match the particulars of designated individuals/entities, CIPL 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 their 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. CIPL 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, CIPL 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. CIPL 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 CIPL are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by CIPL are held by the designated individuals/entities. This verification would be completed within 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 section 51A 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 CIPL 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 CIPL. CIPL 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 CIPL. 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.

Jurisdictions that do not or insufficiently apply the FATF Recommendations:

FATF Secretariat after conclusion of each of its plenary, releases public statements and places jurisdictions under increased monitoring to address strategic deficiencies in their regimes to counter money laundering, terrorist financing, and proliferation financing risks. In this regard, FATF Statements circulated by SEBI from time to time, and publicly available information, for identifying countries, which do not or insufficiently apply the FATF Recommendations, shall be considered by CIPL. CIPL shall take into account the risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statements

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 CIPL through SEBI.

2.12. Reporting to Financial Intelligence Unit-India

2.12.1 In terms of the PML Rules, CIPL is 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, Tower 2, Jeevan Bharati Building,

Connaught Place,

New Delhi-110001.

Telephone : 91-11-23314429, 23314459

91-11-23319793(Helpdesk) Email:helpdesk@fiuindia.gov.in

(For FINnet and general queries)

ctrcell@fiuindia.gov.in

(For Reporting Entity / Principal Officer registration related queries)

complaints@fiuindia.gov.in

Website: <http://fiuindia.gov.in>

2.12.2 CIPL 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, CIPL shall adhere to the following:

a) The Cash Transaction Report (CTR) (wherever applicable) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

b) 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.

c) The Non Profit Organization Transaction Reports (NTRs) for each month shall be submitted to FIU-IND by 15th of the succeeding month. Non-profit organization means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013)

d) The Principal Officer will be responsible for timely submission of CTR, STR and NTR to FIU-IND;

e) Utmost confidentiality shall be maintained in filing of CTR, STR and NTR to FIU-IND.

f) No nil reporting needs to be made to FIU-IND in case there are no cash/ suspicious/ non – profit organization transactions to be reported.

2.12.3 CIPL shall not put any restrictions on operations in the accounts where an STR has been made. CIPL and its 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 CIPL, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, , shall file STR if CIPL has reasonable grounds to believe that the transactions involve proceeds of crime.

2.13. Designation of officers for ensuring compliance with provisions of PMLA

2.13.1 Appointment of a Principal Officer:

2.13.1.1 To ensure that CIPL properly discharges its 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.

Mr. Prakash Nayak, is appointed as Principal Officer on 16.01.2018. The details of his appointment has been intimated to the Financial Intelligence Unit, India (FIU - IND) vide CIPL letter dated 16.01.2018.

Names, designation and addresses (including email addresses) in case of change in ‘Principal Officer’ including any changes therein shall also be intimated to the Office of the Director-FIU. As a matter of principle, ‘Principal Officer’ of CIPL will be of a sufficiently senior position and is able to discharge the functions with independence and authority.

2.13.2 Appointment of a Designated Director:

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

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

- a) the Managing Director or a Whole-Time Director duly authorized by the Board of Directors if the reporting entity is a company,
- b) the managing partner if the reporting entity is a partnership firm,
- c) the proprietor if the reporting entity is a proprietorship firm,
- d) the managing trustee if the reporting entity is a trust,
- e) a person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
- f) such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.”

2.13.2.2 In terms of Section 13 (2) of the PMLA, the Director, FIU – IND can take appropriate action, including levying monetary penalty, on the Designated Director for failure of CIPL to comply with any of its AML/CFT obligations.

2.13.2.3 Mr.Satish Kumar Dutt, Director is appointed as the Designated Director and the details are reported to FIU – IND on August 11, 2014.

2.14. Employees’ Hiring/Employee’s Training/ Investor Education

2.14.1 Hiring of Employees

2.14.1.1 CIPL shall have adequate screening procedures in place to ensure high standards when hiring employees. They shall identify the key positions within its own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

2.14.2 Employees’ Training/ Certification requirements:

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

Composite Investments shall ensure that the employees have NISM certifications mandated by SEBI/Exchanges before handling their respective profile. All employees who operate trading terminals shall compulsorily have certifications on SORM/Equity Derivatives/ Currency Derivatives / Commodity Derivatives as per SEBI guidelines.

Compliance Officer shall have NISM Series III certification.

Composite shall ensure that no employee shall operate terminal without having a valid NISM certificate. Every such employee shall renew the certification before the expiry of its validity failing which he shall not be allowed to operate the terminal.

2.14.3 Investors Education

2.14.3.1 Implementation of AML/CFT measures requires CIPL to demand certain information from investors which may be of personal nature or has 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 client with regard to the motive and purpose of collecting such

information. There is, therefore, a need for CIPL to sensitize its clients about these requirements as the ones emanating from AML and CFT framework. CIPL shall prepare specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT programme.

3. Other principles

CIPL shall ensure the following:

- a) CIPL shall ensure that the content of these Directives are understood by all staff members
- b) CIPL will regularly review the policies and procedures on the prevention of ML and TF on an annual basis to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person doing such a review shall be different from the one who has framed such policies and procedures
- c) CIPL will adopt client acceptance policies and procedures which are sensitive to the risk of ML and TF
- d) CIPL will 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
- e) CIPL have in system a place for identifying, monitoring and reporting suspected ML or TF transactions to the law enforcement authorities; and
- f) CIPL will develop staff members’ awareness and vigilance to guard against ML and TF

This revised policy was approved at the Board meeting of Composite Investments Private Limited held on 25th June 2024

For Board of Directors of Composite Investments Private Limited

Sd/-
(Mukesh P Patel)
Directors

Sd/-
(Satish Kumar Dutt)

Annexure A - CIPL Client On boarding and Periodical Review Policy
Encompassing
Client acceptance policies and procedures/ Due diligence measures on a risk sensitive basis/ Risk
assessment and categorisation

Client onboarding Process at CIPL

- When individual client account opening form is received, all requirements under CKYCR and KRA shall be completed
- When non-individual client account opening form is received, all requirements under KRA shall be completed. As and when CKYCR starts accepting non-individual clients, CKYCR process shall be completed even for non-individual clients
- CIPL will use the Permanent Account number (PAN) allotted by the Indian Income Tax Department as the main identifier for the identity of all individuals. The PAN as provided shall be independently verified from the Income Tax Database/ databases of other entities authorised by the Income Tax department.
- All processes like in-person verification, verification of copies against originals, and all other requirements of KRA and CKYCR shall be met at all times by CIPL diligently

A public database search of the individual (in case of individual clients) and beneficial owners/ senior management in case of non-individuals clients shall be conducted at the following places:

- PAN number search on Google
- Search on Stock exchange provided lists
- Search on whatchoutinvestors.com
- Search on UN databases
- Search in any other commercial database that CIPL may subscribe to

The search shall ensure that identity of the client does not match 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 agency worldwide.

If any alerts are generated during the search, then matter shall be escalated to Principal Officer to take a decision whether to open the account or not.

Income and networth details shall be taken for all clients on a self declaration basis. In case of clients trading on derivatives, documentary evidence of financial details as prescribed under SEBI Circular MIRSD/SE/Cir-19/2009 dated 03-Dec-2009 as modified/ updated/ reissued shall be taken.

Where the above details are not available, the account shall not be opened

Risk categorisation

All clients, at the time of onboarding shall be classified in low, medium and high risk categories based on the following parameters;

- Meets all four parameters - High Risk
- Meets three parameters - Medium Risk
- Meets two or less parameters - Low risk

- Parameter 1(Location) - If the clients' location (registered office address, correspondence addresses and other addresses if applicable) is out of India in any of the high risk jurisdictions as defined by FATF

- Parameter 2(nature of business activity) - If the client is dealing in derivatives segment
- Parameter 3(Trading turnover) - If the turnover of the client is not commensurate with the income/ net worth as provided to CIPL
- Parameter 4(Manner of making payment for transactions undertaken) - if client attempts to make payments from accounts other than its own bank accounts

Persons authorised to trade on behalf of the client

Where an individual client has given authority to another person who is not a relative to trade on its behalf, the matter shall be escalated to Principal Officer

Where a non-individual client has given authority to another person who is not an employee/ office bearer to trade on its behalf, the matter shall be escalated to Principal Officer

In case the authority is given to a SEBI Registered Intermediary like Portfolio Manager or Investment Advisor, the SEBI registration details of such intermediary shall be kept on record.

Client KYC periodic review at CIPL

- the KYC of all clients shall be reviewed and updated on a five yearly basis
- For CSC and High Risk Clients, the KYC shall be reviewed and updated every three years
- For PEP, the KYC shall be reviewed and updated every two years