Last Updated: April 2023

# ANTI MONEY LAUNDERING POLICY

1. **Background and Coverage**

This policy covers all businesses which are part of 360 ONE Group, which do not have their own separate Anti-Money Laundering (AML) Policy, but where a Group entity is acting as a SEBI registered intermediary and / or is subject to the SEBI AML / Know your Client (KYC) guidelines. Hence, it covers, broadly, the Distribution, Advisory, Broking, Depository Participant, Investment Banking and Trust Services businesses, which 360 ONE WAM Ltd carries on through itself or through any of its various subsidiaries and group companies. Hence, the term '360 ONE' shall cover all companies / businesses within the 360 ONE group covered by this Policy. The Lending and Asset Management businesses within 360 ONE Group have their own AML Policies.

2**. Prevention of Money Laundering Act, 2002**

The Prevention of Money Laundering Act, 2002 has come into effect from 1 July 2005. The relevant Notifications / Rules under the said Act have been published in the Gazette of India on July 1, 2005. This Policy now incorporates the changes in the **Prevention of Money Laundering Act (PMLA) Maintenance of Records Rules 2005** made by the Government by publishing in the Official Gazette of India on March 7, 2023.

Securities and Exchange Board of India (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). SEBI has also issued a Master SEBI/ HO/ MIRSD/ DOP/ CIR/ P/ 2019/113October 15, 2019 to all intermediaries registered with SEBI u/s 12 of the SEBI Act providing Guidelines on Anti money Laundering Standards (Guidelines). This Master circular consolidates all the requirements/instructions issued by SEBI with regard to AML/CFT till January 31 2010 and supersedes the earlier circulars, dated September 01, 2009, December 19, 2008, March 20, 2006 and January 18, 2006. This Master Circular is divided into two parts; the first part is an overview on the background and essential principles that concern combating money laundering (ML) and terrorist financing (TF). The second part provides a detailed account of the procedures and obligations to be followed by all registered intermediaries to ensure compliance with AML/CFT directives. Being registered intermediaries, these businesses need to ensure that the amount transacted by Clients through 360 ONE is through legitimate sources only and does not involve and is not designated for the purpose of any contravention or evasion of the provisions of the Income Tax Act, 1961, Prevention of Corruption Act, 1988, any anti-money laundering legislation and/or any other Applicable Law in force and also any laws enacted by the Government of India from time to time or any rules, regulations, notifications or directions issued thereunder.

Updation / Modification to any requirement specified herein pursuant to amendment to any regulations / guidelines / rule shall automatically deem to form part of this policy.

**3. SEBI GUIDELINES ON ANTI MONEY LAUNDERING:**

SEBI has issued various guidelines on Know Your Customer (KYC) standards and AML (Anti-Money Laundering) Measures. Securities and Exchange Board of India's (SEBI) Guidelines / Circulars on Anti Money Laundering Standards –

a) Prevention of Money Laundering Act, 2002 (PMLA), as amended and Rules notified there under ;
b) SEBI circular issued on Anti Money Laundering measures including Master circular of 2018.
c) SEBI clarification on KYC norms of April 24, 2020
The SEBI Guidelines/Circulars are in the context of the recommendations made by the Financial Action Task Force (FATF) on anti-money laundering standards. Compliance with these standards by all intermediaries in the country has become imperative. These Guidelines lay down the minimum requirements / disclosures to be made in respect of Clients.

**Objective**
The objective of this policy is to:

· Create awareness and provide clarity on KYC standards and AML measures;

· Outline the obligations of 360 ONE Group under PMLA;

· Align its operations with international standards and practices;

· Provide a framework from which 360 ONE can develop systems and procedures that are appropriate to their business;

· Maintain uniform practices to ensure that IIFLW adhere to minimum requirement laid out in this guidance note by SEBI. It is obligatory for every employee, at all levels, to go through this Circular, understand the provisions, and co-operate in the implementation of the procedures. For any clarifications on this subject, at any point of time, you should contact the Principal Officer of IIFLW under the Prevention of Money Laundering Act

**4. IMPORTANT PROVISIONS OF THE PREVENTION OF MONEY LAUNDERING ACT AND THE RULES MADE THEREUNDER:**

**IMPORTANT PROVISIONS OF THE ACT**
**Section 3:** Offence of Money Laundering : "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering".
Explanation.—For the removal of doubts, it is hereby clarified that,—
(i) a person shall be guilty of offence of money-laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime, namely:
(a) concealment; or
(b) possession; or
(c) acquisition; or
(d) use; or
(e) projecting as untainted property; or
(f) claiming as untainted property, in any manner whatsoever;
(ii) the process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or

claiming it as untainted property in any manner whatsoever.

**Rule (3A)** of the PMLA Rules has been inserted with respect to implementation of policies by groups. Groups are required to implement group-wide policies for the purpose of discharging obligations under the provisions of Chapter IV of the Prevention of Money-laundering Act, 2002

Rule 2 Clause (cba), 'Group' has been defined to have the same meaning as in Section 286(9)(e) of the Income Tax Act, 1961, which reads as under:

"Group" includes a parent entity and all the entities in respect of which, for the reason of ownership or control, a consolidated financial statement for financial reporting purposes, (i) is required to be prepared under any law for the time being in force or the accounting standards of the country or territory of which the parent entity is resident; or
ii) would have been required to be prepared had the equity shares of any of the enterprises were listed on a stock exchange in the country or territory of which the parent entity is resident.

**Section 4 :** Punishment for Money Laundering : Whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than three years but which may extent to seven years and shall also be liable to fine
Provided that where the proceeds of crime involved in money-laundering relates to any offence specified under paragraph 2 of Part A of the Schedule, the provisions of this section shall have effect as if for the words "which may extend to seven years", the words "which may extend to ten years" had been substituted.

**Section 11A. Verification of identity by reporting entity.**

(1) Every reporting entity shall verify the identity of its clients and the beneficial owner, by-
(a) authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 if the reporting entity is a banking company; or
(b) offline verification under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ; or
(c) use of passport issued under section 4 of the Passports Act, 1967 ; or
(d) use of any other officially valid document or modes of identification as may be notified by the Central Government in this behalf:
Provided that the Central Government may, if satisfied that a reporting entity other than banking company, complies with such standards of privacy and security under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, and it is necessary and expedient to do so, by notification, permit such entity to perform authentication under clause (a):

Provided further that no notification under the first proviso shall be issued without consultation with the Unique Identification Authority of India established under sub-section (1) of section 11 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the appropriate regulator.

(2) If any reporting entity performs authentication under clause (a) of sub-section (1), to verify the identity of its client or the beneficial owner it shall make the other modes of identification under clauses (b), (c) and (d) of sub-section (1) also available to such client or the beneficial owner.

(3) The use of modes of identification under sub-section (1) shall be a voluntary choice of every client or beneficial owner who is sought to be identified and no client or beneficial owner shall be denied services for not having an Aadhaar number.
(4) If, for identification of a client or beneficial owner, authentication or offline verification under clause (a) or clause (b) of sub-section (1) is used, neither his core biometric information nor his number shall be stored.
(5) Nothing in this section shall prevent the Central Government from notifying additional safeguards on any reporting entity in respect of verification of the identity of its client or beneficial owner.
Explanation.-The expressions "Aadhaar number" and "core biometric information" shall have the same meanings as are respectively assigned to them in clauses (a) and ( j) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

As per clarification issued by SEBI in their circular SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated April 24, 2020:
eSign service is an online electronic signature service that can facilitate an Aadhaar holder to forward the document after digitally signing the same provided the eSign signature framework is operated under the provisions of Second schedule of the Information Technology Act and guidelines issued by the controller.

b. In terms of PML Rule 2 (1) (cb) “equivalent e-document” means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature, including documents issued to the Digital Locker account of the investor as per Rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

c. Section 5 of the Information Technology Act, 2000 recognizes electronic signatures (which includes digital signature) and states that where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of a digital signature affixed in such manner as prescribed by the Central Government. Therefore, the eSign mechanism of Aadhaar (using OTP) shall be accepted in lieu of wet signature on the documents provided by the investor. Even the cropped signature affixed on the online KYC form under eSign shall also be accepted as valid signature.

**Section 12 : -Reporting entity to maintain records**
(1) Every reporting entity shall—
(a) maintain a record of all transactions, including information relating to transactions covered under clause (b) in such manner as to enable it to reconstruct individual transactions;
(b) furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;
(e) maintain record of documents evidencing identity of its clients and beneficial owners as well as account files and business correspondence relating to its clients.
(2) Every information maintained, furnished or verified, save as otherwise provided under any

law for the time being in force, shall be kept confidential.
(3) The records referred to in clause (a) of sub-section (1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.
(4) The records referred to in clause (e) of sub-section (1) shall be maintained for a period of five years after the business relationship between a client and the reporting entity has ended or the account has been closed, whichever is later.
(5) The Central Government may, by notification, exempt any reporting entity or class of reporting entities from any obligation under this Chapter.
12A. Access to information.—
(1) The Director may call for from any reporting entity any of the records referred to in section 11A, sub-section (1) of section 12, sub-section (1) of section 12AA and any additional information as he considers necessary for the purposes of this Act.
(2) Every reporting entity shall furnish to the Director such information as may be required by him under sub-section (1) within such time and in such manner as he may specify.
(3) Save as otherwise provided under any law for the time being in force, every information sought by the Director under sub-section (1), shall be kept confidential.
12AA.(1) Every reporting entity shall, prior to the commencement of each specified transaction,——
(a) verify the identity of the clients undertaking such specified transaction by authentication under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 in such manner and subject to such conditions, as may be prescribed: Provided that where verification requires authentication of a person who is not entitled to obtain an Aadhaar number under the provisions of the said Act, verification to authenticate the identity of the client undertaking such specified transaction shall be carried out by such other process or mode, as may be prescribed;
(b) take additional steps to examine the ownership and financial position, including sources of funds of the client, in such manner as may be prescribed;
(c) take additional steps as may be prescribed to record the purpose behind conducting the specified transaction and the intended nature of the relationship between the transaction parties.
(2) Where the client fails to fulfil the conditions laid down under sub-section (1), the reporting entity shall not allow the specified transaction to be carried out.
(3) Where any specified transaction or series of specified transactions undertaken by a client is considered suspicious or likely to involve proceeds of crime, the reporting entity shall increase the future monitoring of the business relationship with the client, including greater scrutiny or transactions in such manner as may be prescribed.
(4) The information obtained while applying the enhanced due diligence measures under subsection
(1) shall be maintained for a period of five years from the date of transaction between a client and the reporting entity.
Explanation.—For the purposes of this section, "specified transaction" means— .
(a) any withdrawal or deposit in cash, exceeding such amount;
(b) any transaction in foreign exchange, exceeding such amount;
(c) any transaction in any high value imports or remittances;
(d) such other transaction or class of transactions, in the interest of revenue or where there is a high risk or money-laundering or terrorist financing, as may be prescribed.

Section 13 : Powers of Director to Impose Fine :
(1) The Director may, either of his own motion or on an application made by any authority, officer or person, make such inquiry or cause such inquiry to be made, as he thinks fit to be necessary, with regard to the obligations of the reporting entity, under this Chapter.
(1A) If at any stage of inquiry or any other proceedings before him, the Director having regard to the nature and complexity of the case, is of the opinion that it is necessary to do so, he may direct the concerned reporting entity to get its records, as may be specified, audited by an accountant from amongst a panel of accountants, maintained by the Central Government for this purpose
(3) Save as otherwise provided under any law for the time being in force, every information sought by the Director under sub-section (1), shall be kept confidential.
(IB) The expenses of, and incidental to, any audit under sub-section (1A) shall be borne by the Central Government.;
(2) If the Director, in the course of any inquiry, finds that a reporting entity or its designated director on the Board or any of its employees has failed to comply with the obligations under this Chapter, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may-
(a) issue a warning in writing; or
(b) direct such reporting entity or its designated director on the Board or any of its employees, to comply with specific instructions; or
(c) direct such reporting entity or its designated director on the Board or any of its employees, to send reports at such interval as may be prescribed on the measures it is taking; or
(d) by an order, impose a monetary penalty on such reporting entity or its designated director on the Board or any of its employees, which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.
(3) The Director shall forward a copy of the order passed under sub-section (2) to every banking company, financial institution or intermediary or person who is a party to the proceedings under that sub-section. Explanation. - For the purpose of this section, "accountant" shall mean a chartered accountant within the meaning of the Chartered Accountants Act, 1949.

**RULES MADE UNDER THE PREVENTION OF MONEY LAUNDERING ACT:**

Prevention of Money-laundering (Maintenance of Records) Rules, 2005.
Rule 3 : Maintenance of records :
Maintenance of records of transactions (nature and value)
(1) Every reporting entity shall maintain the record of all transactions including, the record of
(A) all cash transactions of the value of more than rupees ten lakhs 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;
(BA) all transactions involving receipts by non-profit organisations of value more than rupees ten lakh, 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-
(i) deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:
(a) cheques including third party cheques, pay orders, demand drafts, cashiers cheques or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits, or
(b) travellers cheques, or
(c) transfer from one account within the same banking company, financial institution and intermediary, as the case may be, including from or to Nostro and Vostro accounts, or
(d) any other mode in whatsoever name it is referred to;
(ii) credits or debits into or from any non-monetary accounts such as d-mat account, security account in any currency maintained by the banking company, financial institution and intermediary, as the case may be;
(iii) money transfer or remittances in favour of own clients or non-clients from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:-
(a) payment orders, or
(b) cashiers cheques, or
(c) demand drafts, or
(d) telegraphic or wire transfers or electronic remittances or transfers, or
(e) internet transfers, or
(f) Automated Clearing House remittances, or
(g) lock box driven transfers or remittances, or
(h) remittances for credit or loading to electronic cards, or
(i) any other mode of money transfer by whatsoever name it is called;
(iv) loans and advances including credit or loan substitutes, investments and contingent liability by way of:
(a) subscription to debt instruments such as commercial paper, certificate of deposits, preferential shares, debentures, securitized participation, inter bank participation or any other investments in securities or the like in whatever form and name it is referred to, or
(b) purchase and negotiation of bills, cheques and other instruments, or
(c) foreign exchange contracts, currency, interest rate and commodity and any other derivative instrument in whatsoever name it is called, or
(d) letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;
(v) collection services in any currency by way of collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.
(E) all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India;
(F) all purchase and sale by any person of immovable property valued at fifty lakh rupees or more that is registered by the reporting entity, as the case may be.

**Rule 4 Records containing information:**

The records referred above shall contain the following information:
the nature of transactions b) the amount of the transaction and the currency in which it was denominated c) the date on which the transaction was conducted and d) the parties to the transaction.

**Rule 5 : Procedure and manner of maintaining information:** 1) Every banking company, financial institution and intermediary as the case may be shall maintain information in respect of transactions with its client referred to in rule 3 in hard and soft copies in accordance with the procedure and manner as may be specified by the RBI or the SEBI as the case may be from time to time. 2) Every banking company, financial institution and intermediary shall evolve an internal mechanism for maintaining such information in such form and at such interval as may be specified by the RBI or the SEBI as the case may be, from time to time. 3) It shall be the duty of every banking company, financial institution and intermediary as the case may be to observe the procedure and manner of maintaining information as specified by the RBI or the SEBI as the case may be under sub-rule (1).

**Rule 9. Client Due Diligence.**

The regulations require that:

(1) Every reporting entity shall

(a) at the time of commencement of an account-based relationship-

(i) identify its clients, verify their identity, obtain information on the purpose and intended nature of the business relationship; and

(ii) determine whether a client is acting on behalf of a beneficial owner, and identify the beneficial owner and take all steps to verify the identity of the beneficial owner: Provided that where the Regulator is of the view that money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business, the Regulator may permit the reporting entity to complete the verification as soon as reasonably practicable following the establishment of the relationship; and

(b) in all other cases, verify identity while carrying out:

(i) transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, or

(ii) any international money transfer operations.

Provided that where a client is subscribing or dealing with depository receipts or equity shares, issued or listed in jurisdictions notified by the Central Government, of a company incorporated in India, and it is acting on behalf of a beneficial owner who is a resident of such jurisdiction, the determination, identification and verification of such beneficial owner, shall be as per the norms of such jurisdiction and nothing in the sub-rules (3) to (9) of these rules shall be applicable for due-diligence of such beneficial owner.

Explanation. - For the purposes of this proviso, the expression "equity share" means a share in the equity share capital of a company and equity share capital shall have the same meaning as assigned to it in the Explanation to section 43 of the Companies Act, 2013.

(1A) Subject to the provisions of sub-rule (1), every reporting entity shall within ten days after the commencement of an account-based relationship with a client, file the electronic copy of the client's KYC records with the Central KYC Records Registry;

(1B) The Central KYC Records Registry shall process the KYC records received from a reporting entity for de-duplicating and issue a KYC Identifier for each client to the reporting entity, which shall communicate the KYC Identifier in writing to their client;

(1C) Where a client, for the purposes of clause (a) and clause (b), submits a KYC Identifier to a reporting entity, then such reporting entity shall retrieve the KYC records online from the Central KYC Records Registry by using the KYC Identifier and shall not require a client to submit the same KYC records or information or any other additional identification documents or details, unless -

(i) there is a change in the information of the client as existing in the records of Central KYC Records Registry;
(ii) the current address of the client is required to be verified;
(iii) the reporting entity considers it necessary in order to verify the identity or address of the client, or to perform enhanced due diligence or to build an appropriate risk profile of the client.
(1D) A reporting entity after obtaining additional or updated information from a client under subrule (1C), shall as soon as possible furnish the updated information to the Central KYC Records Registry which shall update the existing KYC records of the client and the Central KYC Records Registry shall thereafter inform electronically all reporting entities who have dealt with the concerned client regarding updation of KYC record of the said client.
(1F) A reporting entity shall not use the KYC records of a client obtained from the Central KYC Records Registry for purposes other than verifying the identity or address of the client and shall not transfer KYC records or any information contained therein to any third party unless authorised to do so by the client or by the Regulator or by the Director;
(1G) The regulator shall issue guidelines to ensure that the Central KYC records are accessible to the reporting entities in real time.
(2) For the purpose of clause (a) of sub-rule (1), a reporting entity may rely on a third party subject to the conditions that—
(a) the reporting entity immediately obtains necessary information of such client due diligence carried out by the third party;
(b) the reporting entity takes 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;
(c) the reporting entity is 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;
(d) the third party is not based in a country or jurisdiction assessed as high risk;
(e) the reporting entity is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable; and
(f) where a reporting entity relies on a third party that is part of the same financial group, the Regulator may issue guidelines to consider any relaxation in the conditions (a) to (d).
(3) The beneficial owner for the purpose of sub-rule (1) shall be determined as under—
(a) where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means. Explanation.—For the purpose of this sub-clause—
1. Controlling ownership interest" means ownership of or entitlement to more than twentyfive per cent. of shares or capital or profits of the company;
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;
(b) where the client is a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen per cent. of capital or profits of the partnership;
(c) where the client is an unincorporated association or body of individuals, the beneficial

owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of such association or body of individuals;
(d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;
(e) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per cent. 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; and
(f) where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.
(4)Where the client is an individual, he shall for the purpose of sub-rule (1) submit to the reporting entity, (a) the Aadhaar number where,
(i) he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of 2016); or
(ii) he decides to submit his Aadhaar number voluntarily to a banking company or any reporting entity notified under first proviso to sub-section (1) of section 11A of the Act; or
(aa) the proof of possession of Aadhaar number where offline verification can be carried out; or
(ab) the proof of possession of Aadhaar number where offline verification cannot be carried out or any officially valid document or the equivalent e-document thereof containing the details of his identity and address; and
(b) the Permanent Account Number or the equivalent e-document thereof or Form No. 60 as defined in Income-tax Rules, 1962; and
(c) such other documents including in respect of the nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the reporting entity:
Provided that if the client does not submit the Permanent Account Number, he shall submit one certified copy of an 'officially valid document' containing details of his identity and address, one recent photograph and such other documents including in respect of the nature or business and financial status of the client as may be required by the reporting entity.
Explanation. - Obtaining a certified copy by reporting entity shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity in a manner prescribed by the regulator.
(5) Notwithstanding anything contained in sub-rules (4) and as an alternative thereto , an individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account: Provided that
(i) the designated officer of the banking company, while opening the small account, certifies under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;

Provided that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail

(ii) the small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place;

(iii) the small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty-four months;

(iv) the small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established as per the provisions of sub-rule (4);

(v) the foreign remittance shall not be allowed to be credited into the small account unless the identity of the client is fully established as per provision of sub-rule (4):

(6) Where the client is a company, it shall for the purposes of sub-rule (1), submit to the reporting entity the certified copies of the following documents or the equivalent edocuments thereof, namely:-

(i) Certificate of incorporation;

(ii) Memorandum and Articles of Association;

(iii) Permanent Account Number of the company;

(iii) a resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and

(iv) a resolution from the Board of Directors and power of attorney granted to its managers, officers or employees, as the case may be, to transact on its behalf; and

(v) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on the company's behalf;

(vi) the names of the relevant persons holding senior management position; and

(vii) the registered office and the principal place of its business, if it is different

(7) Where the client is a partnership firm, it shall, for the purposes of sub-rule (1), submit to the reporting entity the certified copies of the following documents or the equivalent edocuments

thereof, namely: -

(i) registration certificate;

(ii) partnership deed;

(iii) an officially valid document in respect of the person holding an attorney to transact on its behalf.

(iv) the names of all the partners and address of the registered office, and the principal place of its business, if it is different

(8) Where the client is a trust shall, for the purposes of sub-rule (1) submit to the reporting

entity the certified copies of the following documents or the equivalent e-documents thereof, namely:-
(i) registration certificate;
(ii) trust deed; and
(iii) Permanent Account Number or Form No.60 of the trust; and
(iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf;
(v) the names of the beneficiaries, trustees, settlor and authors of the trust and the address of the registered office of the trust; and
(vi) list of trustees and documents as are required for individuals under sub-rule (4) for those discharging role as trustee and authorised to transact on behalf of the trust

(9) Where the client is an unincorporated association or a body of individuals,it shall submit to the reporting entity of the following documents or the equivalent e-documents thereof, namely:
(i) resolution of the managing body of such association or body of individuals;
(ii) Permanent account number or Form No.60 of the unincorporated association or a body of individuals;
(iii) power of attorney granted to him to transact on its behalf; and
(iv) such documents as are required for an individual under sub-rule (4) relating to beneficial owner, managers, officers or employees, as the case may be, holding an attorney to transact on its behalf;
(v) such information as may be required by the reporting entity to collectively establish the existence of such association or body of individuals.

9A) Every Banking Company or Financial Institution or intermediary, as the case may be, 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 a reporting entity has ended or the account has been closed, whichever is later.

(9B) Where the client has submitted any documents for the purpose of sub-rule (1), it shall submit to the reporting entity any update of such documents, for the purpose of updating the records mentioned under sub-rules (4),(5),(6),(7),(8) or (9), as the case may be, within 30 days of such updation

“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);

(10) Where the client is a juridical person, the reporting entity shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

(11) No reporting entity shall allow the opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

(12) (i) Every reporting entity shall exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with their knowledge of the client, his business and risk profile and where necessary, the source of funds.

(ii) 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, the reporting entity 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.

(iii) The reporting entity 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 at appropriate times or as may be specified by the regulator, taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained.

(13) (i) Every reporting entity shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, and products, services, transactions or delivery channels that is consistent with any national risk assessment conducted by a body or authority duly notified by the Central Government.

(ii) The risk assessment mentioned in clause (i) shall -

(a) be documented;

(b) consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;

(c) be kept up to date; and

(d) be available to competent authorities and self-regulating bodies.

(14) (i) The regulator shall issue guidelines incorporating the requirements of sub-rules (1) to (13) above and may prescribe enhanced or simplified measures to verify the client's identity taking into consideration the type of client, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved.

Explanation. - For the purpose of this clause, simplified measures are not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply or where the risk identified is not consistent with the national risk assessment.

(ia) The guidelines issued under clause (i) shall also include appropriate-

(A) exemptions, limitations and conditions and alternate and viable means of identification, to provide account based services to clients who are unable to undergo biometric authentication;

(B) relaxation for continued operation of accounts for clients who are unable to provide Permanent Account Number or Form No. 60; and

(C) exemption, limitations and conditions and alternate and viable means of identification, to provide account based services of clients who are unable to undergo Aadhaar authentication for receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other subsidies, Benefits and Services) Act, 2016 (18 of

2016); owing to injury, illness or infirmity on account of old age or otherwise, and such like causes.";

(ii) Every reporting entity shall formulate and implement a Client Due Diligence Programme, incorporating the requirements of sub-rules (1) to (13), sub-rule (15) and sub-rule (17) and guidelines issued under clause (i) and (ia).

(iii) the Client Due Diligence Programme shall include policies, controls and procedures, approved by the senior management, to enable the reporting entity to manage and mitigate the risk that have been identified either by the reporting entity or through national risk assessment.

(15) Where the client has submitted -

(a) his Aadhaar number under clause (a) of sub-rule (4) to the banking company or a reporting entity notified under first proviso to sub-section (1) of section 11A, such banking company or reporting entity shall carry out authentication of the client's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India;

(b) proof of possession of Aadhaar under clause (aa) of sub-rule (4) where offline verification can be carried out, the reporting entity shall carry out offline verification;

(c) an equivalent e-document of any officially valid document, the reporting entity shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issues thereunder and take a live photo as specified under Annexure 1.

(d) any officially valid document or proof of possession of Aadhaar number under clause (ab) of sub-rule (4) where offline verification cannot be carried out, the reporting entity shall carry out verification through digital KYC.

Provided that for a period not beyond such date as may be notified for a class of reporting entity, instead of carrying out digital KYC, the reporting entity pertaining to such class may obtain a certified copy of the proof of possession of Aadhaar number or the officially valid document and a recent photograph where an equivalent e-document is not submitted.

Explanation. - Obtaining a certified copy by the reporting entity shall mean comparing the copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity as per the provisions contained in the Act.;

(16) Every reporting entity shall, where its client submits a proof of possession of Aadhaar Number containing Aadhaar Number, ensure that such client redacts or blacks out his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15).

(17) (i) A client already having an account based relationship with a reporting entity, shall submit his Permanent Account Number or equivalent e-document thereof or Form No.60, on such date as may be notified by the Central Government, failing which the account shall temporarily cease to be operational till the time the Permanent Account Number or Form No. 60 is submitted by the client:

Provided that before temporarily ceasing operations for an account, the reporting entity shall give the client an accessible notice and a reasonable opportunity to be heard.

Explanation. - For the purpose of this clause, "temporary ceasing of operations" in relation to an account means the temporary suspension of all transactions or activities in relation to that account by the reporting entity till such time the client complies with the provisions of this clause;

(ii) if a client having an existing account based relationship with a reporting entity gives in writing to the reporting entity that he does not want to submit his Permanent Account Number or equivalent e-document thereof or Form No.60, as the case may be, the client's account with the reporting entity shall be closed and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the client in the manner as may be determined by the regulator.

(18) In case of officially valid document furnished by the client does not contain updated address, the following documents or their equivalent e-documents thereof shall be deemed to be officially valid documents for the limited purpose of proof of address:-

(a) utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);

(b) property or Municipal tax receipt;

(c) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;

(d) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation:

Provided that the client shall submit updated officially valid document or their equivalent edocuments
thereof with current address within a period of three months of submitting the
above documents.

(19) Where a client has provided his Aadhaar number for identification under clause (a) of sub-rule (4) and wants to provide a current address, different from the address as per the identity information available in the Central Identities Data Repository, he may give a selfdeclaration
to that effect to the reporting entity.

**Rule 10 – Maintenance of records of the identity of clients:**

(1) Every reporting entity shall maintain the physical copy of records of the identity of its clients obtained in accordance with rule 9, after filing the electronic copy of such records with the Central KYC Records Registry.

(2) The records of the identity of clients shall be maintained by a reporting entity in the manner as may be specified by the Regulator from time to time.

(3) Where the reporting entity does not have records of the identity of its existing clients, it shall obtain the records within the period specified by the regulator, failing which the reporting entity shall close the account of the clients after giving due notice to the client.

(4) Explanation. - For the purpose of this rule, the expression "records of the identity of clients" shall include updated records of the identification data, account files and business correspondence.

THE STANDARDS

Scope and Implementation

The scope of this Policy covers the activity of Broker/DP as an intermediary of SEBI under the PMLA who are required to adopt KYC standards.

360 ONE shall maintain a record of all transactions, the nature and value as has been prescribed in the PMLA.

However for the purposes of suspicious transaction reporting apart from ‘transaction

integrally connected', 'transactions remotely connected or related' should also be considered.

These Standards are designed to help business to meet its responsibilities in relation to the prevention of money laundering.

The Standards are based on the Company Policy, the Money Laundering Rules of the Financial Intelligence Unit - India and relevant local guidelines. They cover the three core areas of money laundering prevention:

A. Policy for acceptance of Clients

B. Procedure for identifying the Clients

C. Transaction monitoring and reporting especially Suspicious Transaction Reporting (STR)

The Standards cover all aspects of our business activities from account relationships and the processing of transactions, through to the provision of advice to Clients. Businesses must also consider the application of the Standards in relation to, for example, joint venture activities and outsourced services – particularly when cross border issues are involved.

**Basic Principles and Objectives of Money Laundering Prevention and Compliance:**

To assist in compliance with Indian Legislation, Rules and Regulations, the following basic principles have to be adopted and maintained by 360 ONE :

1. Policies, procedures and controls should be established and maintained which aim to deter people from transacting through 360 ONE, for laundering the proceeds of illegal activities.
2. Satisfactory "Know Your Customer" procedures must be formulated to identify the Clients, the principal beneficial owners and the source of the funds obtained from the investor. It also includes knowing the nature of the business that the investor normally expects to conduct and being alert to transactions that are abnormal within the relationship.
3. 360 ONE has to appoint a Principal Officer to act as the focal point for all activity relating to money laundering, to monitor compliance and to make regular compliance reports to the Board or Senior Management of the IIFLW.
4. The Principal Officer acts as the central point of contact with the law enforcement agencies. He/She may take assistance/guidance from other departments
5. Unexplained, unusual or abnormal transactions which are not in line with the normal expected trend of transactions in the account including transactions suspected of being linked to criminal conduct should be reported to the Principal Officer who should then determine whether a report should be made to the appropriate authority.
6. Reporting lines for suspicious transactions should be clear and unambiguous and all reports should reach the Principal Officer without delay.
7. All staff should have access to information about their statutory responsibilities and relevant staff should be made aware of the anti-money laundering policies and procedures. Relevant staff should be provided with Anti Money Laundering training that helps them to understand the money laundering risks involved in business. Records must be kept regarding persons trained.
8. Records confirming the identity of Clients should be retained for five years following the cessation of the business relationship. The records referred in Rule 3 of Prevention of Money Laundering Rules, 2005 shall be maintained for a period of five years from the date of cessation of the transactions between the Investor and the IIFLW.

**Roles and Responsibilities**

**Business Managers**

The Company heads have primary responsibility for the prevention of money laundering. They are responsible for the development, implementation, maintenance and monitoring of procedures and controls that meet the requirements of India Policy on Money Laundering prevention.

**Designated Director**

The Chief Executive Officer/Executive Director is appointed as the Designated Director for the purpose of AML Laws. The Designated Director is responsible to ensure overall compliance with the obligations imposed on IIFLW under the AML Laws.

**Principal Officer**

The IIFLW shall appoint a Principal Officer who shall be responsible for reporting suspicious transactions to authorities and would act as a central reference point in facilitating onward reporting of suspicious transactions and play an active role in identification and assessment of potentially suspicious transactions.

· Monitoring the effective implementation of AML Policy

· To ensure compliance with Anti Money Laundering Policy, including testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and / or irregular transactions, the quality of reporting suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.

· Reporting of transactions and sharing of information as required under the law

· Liasoning with law enforcement agencies

· Ensuring submission of periodical reports to Top Management. The monthly compliance report shall henceforth mention if any suspicious transactions are being looked into by the respective business groups and if any reporting is to be made to the authorities.

· Providing clarifications / training to staff members on the provisions of the Act, Rules, Guidelines and the policy of the company

**Compliance, Quality Assurance & Risk Control**

Compliance and Risk Management department, directly or through Internal Auditor, is responsible for the general oversight of the operation of the anti-money laundering policy, the effectiveness and integrity of suspicious transaction reporting procedures, and taking reasonable steps to establish and maintain adequate arrangements for money laundering training.

**Anti Money Laundering (AML) Committee**

The AML committee comprises of the following:

1. COO
2. Compliance Officer
3. Head – Risk
4. Executive Director

Quorum of the Committee shall be one-third of the total members or two, whichever is greater/ higher and that the Committee shall meet at such interval(s), time as it may from time to time deem fit.

**All employees**

· To be aware of and understand the guidelines provided in this Policy

· To be vigilant in detecting and reporting all suspicious transactions to their manager.

· To maintain utmost confidentiality on accounts identified as suspicious and not to discuss their suspicions with anyone except their manager.

**Combating Money Laundering**

"Money laundering" is the process by which persons attempt to hide and disguise the true origin and ownership of the proceeds of their illegal activities, thereby avoiding prosecution, conviction and confiscation of the funds generated through illegal acts and means. The term "Money Laundering" is also used when the funds are used for terrorist financing though the origin of the funds may be legitimate.

Basically, the money laundering process involves three stages:

1. Placement - the physical disposal of cash proceeds derived from illegal activity.
2. Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to hamper the audit trail, disguise the origin of such funds and provide anonymity to their owners.
3. Integration - placing the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be legitimate business funds.

Having identified these stages of the money laundering process, IIFLW has to adopt procedures to guard against and report suspicious transactions that occur at any stage.

The ability to launder the proceeds of criminal activity through the financial systems of the world is vital to the success of criminal operations, and therefore India, as one of the world's emerging financial markets, has a vital role to play in combating money laundering. IIFLW being involved in money laundering offences could face prosecution under PMLA leading to reputation and other risks.

Client themselves are better protected if IIFLW is able to protect itself against criminal activity. Failure to prevent the laundering of the proceeds of crime permits criminals to benefit from their actions, thus making crime an attractive proposition.

Adherence to AML policies and procedures should also enhance the fraud prevention measures that IIFLW takes to protect itself and their genuine Clients from losses.

**Money Laundering risk assessments:**

Risks assessment on money laundering is dependent on the kind of customers the IIFLW deals with. Typically, risks are increased if the money launderer can hide behind corporate structures such as limited companies, offshore trusts, special purpose vehicles and nominee arrangements. IIFLW will consider how their customer base and operational systems impact upon the capacity of their staff to identify suspicious transactions.

**Risk classification**

The level of Money Laundering (ML) risks that the IIFLW is exposed to by an investor relationship depends on:

• Type of the customer and nature of business
• Type of product / service availed by the customer
• Country where the Customer is domiciled.

Based on the above criteria, the Clients are classified into various Money laundering Risk levels.

This policy define certain minimum standards of account documentation for all customer relationships, to enable the IIFLW to understand the nature of the customer's business, carry evidence of key data regarding the customer and its principal owners/ signatories and understand the type and level of activity that is to be considered as normal in the customer's account.

Further, 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.

Clients are classified in the following risk categoriesi)

**High Risk / Client of Special Category**

The following Clients are classified as high risk:

a) Non resident clients

b) High Net-worth clients with more than INR 100 Crore of Net worth (not including those with whom client relationship of IIFL Group is more than 2 years)

c) Trust, Charities, NGOs and organizations receiving donations

d) Companies having close family shareholdings or beneficial ownership

e) Politically exposed persons (PEP)

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 countries where the existence / effectiveness of money laundering control is suspect. In addition to following the Financial Action Task Force (FATF) 360 ONE shall also undertake internal assessment of other public information.

h) Non face to face client

i) Clients with dubious reputation as per public information available

**(ii) Low Risk**

All customers that are not High Risk would usually be classified as Low Risk customers.

**(iii) Medium Risk**

Clients who frequently change addresses or display unexpected transaction patterns that increase their money laundering risk may be classified as Medium Risk Customers.

The regulations define "Politically Exposed Persons" (PEPs) as individuals who have been entrusted with prominent public functions by a foreign country, including the heads of States or Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials

Following Risk based KYC procedures are adopted for all clients:

i. Large number of accounts having a common account holder

ii. Unexplained transfers between multiple accounts with no rationale

iii. Unusual activity compared to past transactions

iv. Doubt over the real beneficiary of the account

v. Pay-out/pay-in of funds and securities transferred to /from a third party

vi. Off market transactions especially in illiquid stock and in F & O, at unrealistic prices
vii. Large sums being transferred from overseas for making payments
viii. Inconsistent with the clients' financial background

**KNOW YOUR CUSTOMER (KYC)**

**General**

"Know Your Customer" (KYC) is a fundamental principle of all anti-money laundering controls. It includes identification of the investor, but it also extends to a full understanding of the nature of the business that underlies a relationship. KYC is an ongoing process - it does not end when account opening procedures are completed. Effective KYC can reduce the risk of accounts being used for money laundering, and can help us to identify suspicious transactions.

The more we know about an investor and their business, the better are the chances of identifying changes in their activities that may be grounds for further enquiry, possibly leading to a report to the appropriate authorities. It is therefore essential that adequate information is gathered about the Clients or proposed Clients, and the nature of their activities, when a relationship begins.

Having sufficient information about our investor and making use of that information is the most effective tool used to counter the efforts of laundering the proceeds of crime. In addition to minimizing the risk of being used for illicit activities, adequate KYC information provides protection against frauds, enables suspicious activity to be recognized and protects 360 ONE from reputation and financial risks.

Where the investor is a new investor, account must be opened only after ensuring that pre account opening KYC documentation and procedures are conducted.

A risk-based approach will need to be adopted towards Investor identification in respect of any additional information that might be required in specific cases.

**Application of Commercial Judgment**

360 ONE will follow a risk-based approach to the KYC requirements. Consequently, there will be circumstances when it will be both necessary and permissible to apply commercial judgment to the extent of the initial identification requirements. Decisions will need to be taken on the number of verification parameters within a relationship, the identification evidence required, and when additional checks are necessary.

**The KYC measures would comprise the following:**

**(a) Customer Identification process**

The documentation & information requirements and the procedural aspects for completion of the KYC formalities shall be as prescribed by AML Laws/SEBI/KRA from time to time.

KYC Form shall be submitted by customer along with investment application form. However, an existing customer who is not KYC compliant may submit new KYC Form along with the application form.

In-Person Verification (IPV) of customers shall be performed by the authorized employees of 360 ONE/ CAMS. For IPV process, guidelines prescribed by KRA from time to time shall be followed. In line with the KRA regulations, 360 ONE can place reliance on IPV carried out by any other SEBI registered Intermediary, including AMFI registered distributors.

In case of investment in the name of a minor, the minor will be required to complete KYC formalities on attaining age of majority.

In case of non-individual customers (other than HUF), identification of ultimate beneficial

owner shall be mandatory. The investor shall be required to furnish information about its ultimate beneficial owners as may be prescribed by 360 ONE from time to time taking into consideration the industry practice.

Applications that do not meet the above requirements are liable to be rejected.

In order to enable the Online KYC process for establishing account based relationship with the RI, Investor's KYC can be completed through online / App based KYC, in-person verification through video, online submission of Officially Valid Document (OVD) / other documents under eSign, in the following manner:

i. The investor visits the website/App/digital platform of the RI and fills up the online KYC form and submits requisite documents online.

ii. The name, photograph, address, mobile number, email ID, Bank details of the investor shall be captured online and OVD / PAN / signed cancelled cheque shall be provided as a photo / scan of the original under eSign and the same shall be verified as under:

a. Mobile and email is verified through One Time Password (OTP) or other verifiable mechanism. The mobile number/s of investor accepted as part of KYC should preferably be the one seeded with Aadhaar. (the RI shall ensure to meet the requirements of the mobile number and email as detailed under SEBI circular no. CIR/MIRSD/15/2011 dated August 02,2011)

b. Aadhaar is verified through UIDAIs authentication / verification mechanism. Further, in terms of PML Rule 9 (16), every RI shall, where the investor submits his Aadhaar number, ensure that such investor to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15). 360 ONE shall not store/ save the Aadhaar number of investor in their system. e-KYC through Aadhaar Authentication service of UIDAI or offline verification through Aadhaar QR Code/ XML file can be undertaken, provided the XML file or Aadhaar Secure QR Code generation date is not older than 3 days from the date of carrying out KYC. In terms of SEBI circular No. CIR/MIRSD/29/2016 dated January 22, 2016 the usage of Aadhaar is optional and purely on a voluntary basis by the investor.

c. PAN is verified online using the Income Tax Database.

d. Bank account details are verified by Penny Drop mechanism or any other mechanism using API of the Bank. (Explanation: based on bank details in the copy of the cancelled cheque provided by the investor, the money is deposited into the bank account of the investors to fetch the bank account details and name.) The name and bank details as obtained shall be verified with the information provided by investor.

e. Any OVD other than Aadhaar shall be submitted through Digiocker / under eSign mechanism.

The original seen and verified requirement under SEBI circular no. MIRSD/SE/Cir-21/2011 dated October, 5 2011 for OVD would be met where the investor provides the OVD in the following manner:

i. As a clear photograph or scanned copy of the original OVD, through the eSign mechanism, or;

ii As digitally signed document of the OVD, issued to the DigiLocker by the issuing authority.

i. In-person verification (IPV)/ Video IPV (VIPV) would not be required when the KYC of the investor is completed using the Aadhaar authentication / verification of UIDAI.

ii. IPV / VIPV shall not be required by the RI when the KYC form has been submitted online, documents have been provided through digilocker or any other source which could be verified online.

**5. Features for online KYC App (if and when used)** – As a SEBI registered intermediary, IIFL and its group companies may implement their own Application (App) for undertaking online KYC of investors.

The App shall facilitate taking photograph, scanning, acceptance of OVD through Digilocker, video capturing in live environment, usage of the App only by authorized person of 360 ONE. The App shall

also have features of random action initiation for investor response to establish that the interactions not pre-recorded, time stamping, geo-location tagging to ensure physical location in India etc is also implemented. 360 ONE shall ensure that the process is a seamless, real-time, secured, end-to-end encrypted audiovisual interaction with the customer and the quality of the communication is adequate to allow identification of the customer beyond doubt. 360 ONE shall carry out the liveliness check in order to guard against spoofing and such other fraudulent manipulations. 360 ONE shall, before rolling out and periodically, carry out software and security audit and validation of their App. 360 ONE may have additional safety and security features other than as prescribed above.

**6. Feature for Video in Person Verification (VIPV) for Individuals** – To enable ease of completing IPV of an investor, intermediary may undertake the VIPV of an individual investor through the App. The following process shall be adopted in this regard:

i. 360 ONE through its authorised official, specifically trained for this purpose, may undertake live VIPV of an individual customer, after obtaining his/her informed consent. The activity log along with the credentials of the person performing the VIPV shall be stored for easy retrieval.

ii. The VIPV shall be in a live environment.

iii. The VIPV shall be clear and still, the investor in the video shall be easily recognisable and shall not be covering their face in any manner.

iv. The VIPV process shall include random question and response from the investor including displaying the OVD, KYC form and signature or could also be confirmed by an OTP.

v. 360 ONE shall ensure that photograph of the customer downloaded through the Aadhaar authentication / verification process matches with the investor in the VIPV.

vi. The VIPV shall be digitally saved in a safe, secure and tamper-proof, easily retrievable manner and shall bear date and time stamping.

vii. 360 ONE may have additional safety and security features other than as prescribed above.

**(b) Determining Ultimate Beneficial Owners (UBO):**

As a part of Client Due Diligence (CDD) Process under PMLA 2002 read with PMLA Rules, 2005 each of the SEBI registered entity, is required to obtain sufficient information from their clients in order to identify and verify the identity of persons who beneficially own or control the securities account.

Further, various circulars issued on Anti money laundering requires, Clients (other than Individuals) are required to provide details of Ultimate Beneficial Owner(s) ("UBO(s)") and submit proof of identity (viz. PAN with photograph or any other acceptable proof of identity prescribed in common KYC form) of UBO(s). In order to comply with the above Act/Rules/Regulations & Guidelines, the following CDD process is being implemented by 360 ONE:

**I. Applicability:**

1. Providing information about beneficial ownership will be applicable to the subscriptions received from all categories of Clients except Individuals and a Company listed on a stock exchange or is a majority owned subsidiary of such a Company.

2. Proof of Identity of the UBO such as Name/s, Address & PAN/Passport together with self attested copy along with the 'Ultimate Beneficial Ownership' declaration form is required to be submitted.

**II. Identification Process:**

(A) For Clients other than Individuals or Trusts:

(i) If the investor is an unlisted company, partnership firm or unincorporated association / body of individuals, the beneficial owners are the natural person/s who is/are acting alone or

together, or through one or more juridical person and exercising control through ownership or who ultimately has a controlling ownership interest.
(ii) Controlling ownership interest means ownership of /entitlement to:
a) more than 10% of shares or capital or profits of the juridical person, where juridical person is a company.
b) more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership firm; or
c) 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.
(iii) In cases, where there exists doubt 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 details should be provided of the natural person who is exercising control over the juridical person through other means (i.e. control exercised through voting rights, agreement, arrangements or in any other manner).
(iv)In case no natural person is identified under any of the above criteria, the person who holds the position of senior managing official shall be provided.
(B) For Investor which is a Trust:

e) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, 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 (reduced from 15%);

(Partnership firm and unincorporated body of individuals remain at 15%)

(C) 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.
(D) Applicability for foreign Clients:
Where Foreign Portfolio Clients and Foreign Clients are transacting through 360 ONE KYC shall be undertaken as per requirements specified under various SEBI circulars prescribed from time to time.
In case a person has beneficial ownership or control of the investments then the Company would obtain sufficient information in order to verify the identity of such persons. Wherever it is apparent that the units acquired or maintained through an account are beneficially owned by a person other than the investor, the principal i.e. the beneficial owner would be identified using Investor identification and verification procedures. The identity of the beneficial owner would be identified using reliable, independent source documents, data or information.
**(b) Ongoing Due Diligence :**
Investment Manager shall conduct ongoing due diligence and scrutiny of the transactions in the account of the investor throughout the course of the investment period to ensure that the transactions are being conducted in a consistent manner regarding the profile of the investor, his business and risk profile in relation to the investor's source of funds.
(c) Maintenance of KYC Records:

360 ONE shall take all reasonable steps to ensure that KYC information is collected and kept upto-date, and that identification information is updated when changes occur with respect to the investor. Further the data is required to be maintained for 10 years from the date of closure of accounts.

**Establishing Identity**

What is identity?

Identity generally means a set of attributes which together uniquely identify a natural or legal person. For example, an individual's identity comprises his/her name including all other names used, the residential address at which he/she can be located and his/her photograph. Date of birth is also important as an identifier in support of the name and is essential to law enforcement agencies in an investigation.

Whose Identity Should Be Verified?

Identification evidence should usually be verified for:

- the named account holder(s)/the person in whose name an investment is registered;
- any principal beneficial owner of funds being invested who is not the account holder or named investor;

The failure or refusal by an applicant to provide satisfactory identification evidence within a reasonable time scale and without adequate explanation may lead to a suspicion that the investor is engaged in money laundering. In such circumstances, 360 ONE would consider making
a suspicious activity report.

Identification Procedures: General Principles: 360 ONE shall establish to its satisfaction that they are dealing with an individual or an entity and obtain identification evidence sufficient to establish that the applicant is that individual or entity.

When reliance is being placed on any third party to identify or confirm the identity of any applicant, the overall legal responsibility to ensure that the procedures and evidence obtained are satisfactory rests with the 360 ONE.

It is important that the procedures adopted to verify identity are sufficiently robust whether the procedures are being undertaken face-to-face or remotely.

Reasonable steps should be taken to avoid single or multiple fictitious applications or substitution (impersonation) fraud for the purpose of money laundering.

360 ONE shall implement accepting of Aadhaar and implementation of Central KYC requirements
as notified by the regulators from time to time.

Certification and Copying Identification Documents

A risk-based approach will be adopted towards certification of Documents. For all Clients, 360 ONE would adopt higher levels of verification procedures (such as requesting certified copies
or sighting of originals etc.) to ensure validity of the documents submitted.

Based on materiality and risk, verification of beneficial owners or directors may not be taken for significant and well established entities, companies listed on recognized investment/stock exchanges, government departments or their agencies, government linked companies.

**KYC Reviews**

KYC information should be regularly reviewed following account opening, or the commencement of a relationship, and any significant changes in the investor's activities should be recorded. The frequency of reviews should be determined by the level of risk

associated with the relationship and recorded as part of the investor file data. Higher risk, high value or high volume accounts should, for example, be reviewed at more frequent intervals.
Any shortcomings in KYC information highlighted by a review must be remedied as soon as possible. Steps must be taken to obtain additional information about existing (even longstanding) Clients where it is apparent that existing KYC information is out of date or inadequate.
When the business is notified of, for example, an acquisition being made by an investor company or changes to those controlling the business, this should act as a trigger to update KYC information.

**Identification - General**

Establishing and retaining documentary evidence of the true identity (and address) of investor is a critical part of the KYC regime. It is essential that we are satisfied that Clients are who they claim to be and that they are not conducting business in fictitious names, possibly to disguise their involvement in illicit activity.
Reasonable steps must therefore be taken, by obtaining and verifying sufficient evidence of identity, to be able to show that an investor, or potential investor, is who they claim to be. Where the investor is, or appears to be, acting on behalf of another, sufficient identification evidence must be obtained in respect of both parties. These steps must be taken as soon as possible after contact with an investor or potential investor is made with a view to carrying out a transaction or reaching an understanding to carry out the transaction.
KYC for Specific Investor Categories
The following sections summarise KYC and identification standards for the most common investor categories. For any other (specialised) investor category, not specified below, KYC and identification procedures adopted shall be in line with applicable regulation.
Individual Clients
1. Identification evidence (including evidence of addresses) must be obtained and retained on file, for all parties to an account, including any beneficial owner of funds who may not be a signatory to the account. Identification evidence must also be retained for any intermediate parties where an account is managed or owned by an intermediary.
2. Clear, legible copies of all relevant pages of identification documents must be retained on investor files.
3. Whenever possible, identification evidence should be provided by the investor at a face to face meeting before an account is opened. Where verification of identity cannot be completed face to face, copy of passports or identity cards suitably certified by another correspondent bank, or diplomatic mission, may be acceptable.
Individual Clients - Evidence and Verification of Addresses
Copies of documents and a record of the manner in which address verification was achieved must be retained in Investor files. Only ‘officially valid document’ as prescribed under PMLA (Maintenance of Records) rules 2005, shall be accepted by 360 ONE. Officially valid document in this record shall mean the following:
a. Passport
b. Driving Licence
c. Voters Identity card issued by Election commission of India
d. Job card issued by NREGA duly signed by an officer of the state government of name, address or any other document as notified by the Central Government.
As prescribed under PMLA rules, 360 ONE may at its discretion accept the following documents,

however within three months of submitting such documents shall ensure that the officially valid document is sought and updated in record. The other documents which shall be accepted as proof of address shall mean the following:

a. Utility bill which is not more than two months old of any service provider (electricity, water, telephone, post paid, mobile phone, piped gas);

b. Property or municipal tax receipt;

c. Pension or family pension payment orders (PPO) issued to retired employees by Government Departments or Public Sector Undertakings if they contain the address;

d. Letter of allotment of accommodation from employer issued by State Government or Central government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies, leave and licence agreements with such employers allotting official accommodation.

Individual Clients - Minors and Students

1. In some circumstances, accounts for minors are opened by adult family members. In these circumstances, identity evidence for the guardian, or anyone else operating the account, should be obtained together with a copy of the birth certificate or passport of the minor.

2. For students, evidence of identity and address verification should be obtained in the normal way as far as is possible. Where this proves impractical however, verification can be obtained through a parent or the prospective Investor's college or university.

Trusts, Nominee Companies and Fiduciaries

a. Money launderers may view the anonymity and complex structures associated with some types of Trust arrangement as providing an opportunity to avoid identification procedures and conceal the origin of funds.

b. It is therefore essential to verify the identity of the settlor of the Trust (i.e. the person supplying the funds), those who have control over the funds, beneficiaries, and any person who has authority to remove the Trustees. Exceptionally, identification requirements may be waived for any Trustee who does not operate an account or give instructions relating to fund transfers. Whenever a Trustee is replaced, the identity of the new Trustee should be verified before they are allowed to exercise control over the funds.

c. Whenever funds are received on behalf of a Trust the source of the funds must be properly identified, and the nature of the transaction understood (reasonable exceptions may be allowed in the case of regular receipts from the same, previously identified source).

d. For discretionary and offshore Trusts, the nature and purpose of the Trust as well as the original source of funding must be ascertained.

e. 5. Particular care must be taken when Trusts are set up in offshore locations where strict banking secrecy prevails. Trusts set up in jurisdictions where no money laundering legislation or regulation exists will also warrant additional enquiries and measures. Steps should be taken to obtain written confirmation from the trustees or managers of the Trust that there are no anonymous principals. The original source of the funding should also be established.

f. Any application to open an account or undertake a transaction on behalf of another without the applicant identifying their Trust or nominee capacity should be regarded as suspicious and treated accordingly.

Corporate Investor

1. Companies can be established with the sole purpose of laundering money, or illicit money can be passed through the accounts of otherwise legitimate companies. The KYC process must ensure the company is not merely a 'brass plate' company set up to facilitate money

laundering.
2. For corporate Clients it is essential to identify the ultimate beneficial owners as mentioned in the Policy earlier.

**Powers of Attorney and Third Party Mandates**

1. The authority to deal with assets under a Power of Attorney or Third Party Mandate constitutes a business relationship and therefore any person fulfilling that role must also be identified in the same manner as the primary Investor. A copy of such Power of Attorney must be obtained and verified with the original or copy should be attested by Gazetted officer.
2. New power of attorney for corporate or Trust businesses should always be verified and it is important that the reason for granting the power of attorney is understood and recorded.

Unincorporated Businesses/Partnerships

1. Where they do not already hold personal Bank accounts, identification evidence must be obtained for the principal beneficial owners or controllers of these types of business. This may include identifying signatories to whom significant control has been delegated. Where a formal partnership arrangement exists, a mandate authorising the opening of the account and the issuing of instructions for transactions should be obtained.
2. Evidence of the trading address must be obtained. It must also be established that the business or partnership has a legitimate purpose by, for example, a visit to the trading address to confirm the true nature of the business activities. For established businesses, a copy of the latest report and accounts should be obtained.

**Financial Institutions**

1. It is essential to determine that a financial institution with which a relationship is proposed, is properly constituted, is supervised and regulated by an acceptable regulatory authority and in addition to normal business considerations, is an institution with which we would wish to be associated from a reputational perspective.
2. Discretion should be exercised as to whether these documents should be certified.
3. Consideration should also be given as to whether it is necessary to check the institution with the relevant regulator, a known correspondent in a suitably regulated country.
4. Relationships must not be established with “Shell Banks” that have no physical presence in any country, or with correspondents that allow their accounts to be used by such institutions.

**Financial Institutions Acting as Agents**

Where a Client of the Bank, “A”, acts as an agent for an underlying Client “B”, the identity of both “A” and “B” must be verified in accordance with these Standards. However, a copy of the legal mandate for the Bank to act on behalf of its Investor for investment should be obtained for our records and the same must be verified with the original.

**Enhanced Customer Due Diligence**

For customers that may present a higher risk of money laundering and terrorist financing, enhanced due diligence must be performed.
In addition to performing the customer identification procedure as specified above, any of the following additional measures should also be undertaken, where applicable, for conducting Enhanced CDD:

o To obtain approval of AML committee (approval by majority) for onboarding clients where any world check alert is received or the client is identified as a shell company or a rule based shell company as per lists issued by FIU IND and conduct enhanced due diligence by seeking additional information from customer such as, details of source of funds, financial statements, tax returns and details of occupation or business (where applicable)

o Update of KYC profile for High Risk Clients on periodical basis (if any negative world check report is received) to obtain additional information from customer such as, details of source of funds, financial statement, and details of occupation or business (where applicable).
o To inform designated director about opening of an account by PEP and obtaining designated directors' approval for continuing business relationship with PEP.
o In case a customer becomes PEP subsequently, approval from designated director is to be obtained for continuing existing relationship.
o Monitoring the activities of such customer more closely.

**Additional Measures**

In addition to the CDD process stated above, IIFL has implemented following as a measure to prevent money-laundering:
o No acceptance or remittance/payout in cash. Payout shall be made only through an account payee check or electronic fund transfer through the Customer's registered bank account.
o Non-acceptance of third party payment for investment
o No third party remittance for payout of funds
o Verification of bank account registered in the customer's account
Declaration on the source and legitimacy of funds shall be obtained from the Customers in respect of all investments through pay orders/demand drafts/electronic transfers.

**Monitoring Conduct of the account**

In line with KYC guidelines, 360 ONE will continuously develop and implement appropriate methods of monitoring so that throughout the Investor relationship, suspicious Investor activity can be detected, appropriate action can be taken and reports made to the regulatory authorities in accordance with laid down procedures.

**Record Retention**

In case of any suspicious transaction, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of such transaction. Hence proper record keeping and retention should be adopted. Identification and account opening records must be retained for a period of 5 years after a relationship has ended. Records relating following information should also be retained for a minimum of 5 years:
1. the beneficial owner of the account
2. volume of the funds flowing through the account
3. origin of funds
4. form in which the funds were offered or withdrawn i.e. cheques, wire transfer, drafts.
5. identity of person undertaking the transaction
6. destination of the funds
7. form of instruction and authority
8. The nature of transaction;
9. The amount of the transaction and the currency in which it was denominated;
10. The date on which the transaction was conducted; and
11. The parties to the transaction.

Records may be retained in hard copy, on microchip or computer, or other electronic format. The documents should be kept updated and should be readily and quickly made available to the investigating authorities.
Care should be taken to ensure that transactional records are not lost before the year retention period expires as a direct consequence of automatic data retention constraints. Documentary evidence of any action taken in response to internal and external reports of suspicious

transactions must also be retained for at least 5 years from the closure of accounts. Where it is known that an investigation is ongoing, the relevant records should be retained until the authorities inform the 360 ONE otherwise.

Where business is refused because of a failure to meet these Standards or other local antimoney laundering requirements, a record of the refusal should be retained for years (no record is required where business is refused on purely commercial grounds)

**Wire Transfers/Electronic Fund Transfers**

Particular attention must be paid to the adequacy of information contained in records relating to electronic fund transfer instructions. These offer money launderers the opportunity to speedily disperse funds to different jurisdictions making subsequent tracing and investigation difficult. To assist investigating authorities, all electronic payment messages, both domestic and international should, subject to any technical limitations, contain the full name, account number and address of the ordering Investor and beneficiary in the respective message fields.

Where this information is not contained in electronic payment messages, full records must be retained by the originating office (this does not apply to inter-bank transfers). These records must be retained as stated above

**Cash transactions**

As per the policy, 360 ONE does not entertain cash transactions.

**Monitoring & Reporting of Suspicious Transactions:**

“Suspicious transaction" means a transaction whether or not made in cash, which to a person acting in good faith -

i. gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the Schedule to the Act, regardless of the value involved; or

ii. appears to be made in circumstances of unusual or unjustified complexity; or

iii. appears to have no economic rationale or bonafide purpose; or

iv. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;’.

**Ongoing monitoring of accounts which includes**

i) Identification and detection of apparently abnormal transactions

ii) Generation of necessary reports/alerts based on clients’ profile, nature of business, trading pattern of clients for identifying and detecting such transactions.

These reports/alerts are analyzed to establish suspicion or otherwise for the purpose of reporting such transactions

**Following parameters are used:**

a. Clients whose identity verification seems difficult or clients appear not to cooperate

b. Substantial increase in activity without any apparent cause

c. Large number of accounts having common parameters such as common partners / directors / promoters / address / email address / telephone numbers / introducers or authorized signatories;

d. Transactions with no apparent economic or business rationale

e. Sudden activity in dormant accounts;

f. Source of funds are doubtful or inconsistency in payment pattern;

g. Unusual and large cash deposits made by an individual or business;

h. Transfer of investment proceeds to apparently unrelated third parties;

i. Multiple transactions of value just below the threshold limit of Rs 10 Lacs specified in PMLA so as to avoid possible reporting;

j. Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
k. Purchases made on own account transferred to a third party through off market transactions through DP Accounts;
l. Suspicious off market transactions:
i. Large deals at prices away from the market
ii. Accounts used as 'pass through'. Where no transfer of ownership of securities or trading is occurring in the account and the account is being used only for funds transfers/layering purposes.
iii. All transactions involving receipts by non-profit organizations of value more than rupees ten lakh, or its equivalent in foreign currency;
iv. 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 'Clients of Special Category'. Such clients should 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.
v. Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, file STR if we have reasonable grounds to believe that the transactions involve proceeds of crime.

**H. Reporting of Suspicious Transactions:**

i. All suspicious transactions will be reported to FIU. Member and its employees shall keep the fact of furnishing information in respect of transactions referred to in clause (D) of subrule (1) of rule 3 strictly confidential.
ii. 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 should be made available to auditors and also to SEBI /Stock Exchanges/FIUIND/ Other relevant Authorities, during audit, inspection or as and when required. These records are required to be preserved for Five years as is required under PMLA 2002.
iii. The Principal Officer and related staff members shall have timely access to customer identification data and other CDD information, transaction records and other relevant information. The Principal Officer shall have access to and be able to report to senior management above his/her next reporting level or the Board of Directors.

**Ongoing training to Employees:**

i. Importance of PMLA Act & its requirement to employees through training.
ii. Ensuring that all the operating and management staff fully understands their responsibilities under PMLA for strict adherence to customer due diligence requirements from establishment of new accounts to transaction monitoring and reporting suspicious transactions to the FIU.
iii. Organising suitable training programmes wherever required for new staff, front-line staff, supervisory staff, etc.

J. Audit and Testing of Anti Money Laundering Program.

The Anti Money Laundering program is subject to periodic audit, specifically with regard to testing its adequacy to meet the compliance requirements. The audit/testing is conducted by

Trading Member's own personnel not involved in framing or implementing the AML program. The report of such an audit/testing is placed for making suitable modifications/improvements in the AML program.

**M. Investors Education:**

As the implementation of AML / CFT measures being sensitive subject and requires us to demand and collect certain information from investors which may be of personal in nature or has hitherto never been called for, which information include documents evidencing source of funds / income tax returns / bank records etc. and 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 us to sensitize the clients about these requirements, as the ones emanating from AML and CFT framework. We shall circulate the PMLA Circulars and other specific literature/ pamphlets etc. so as to educate the client of the objectives of the AML/CFT program. The same shall also be emphasized on, in the Investor Awareness Programmes conducted by us at frequent intervals of time. The importance of the same is also made known to them at the time of opening the Account.

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

Freezing of funds, financial assets or economic resources or related services

Section 51A of the Unlawful Activities (Prevention) Act, 1967 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 Central Government has issued an Order dated August 27, 2009 detailing the procedure for the implementation of Section 51A of the UAPA.

In this regard, 360 ONE shall be implement the following procedure laid down in the UAPA order dated August 27, 2009 :

a) On receipt of 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 which SEBI shall forward to all intermediaries;

b) 360 ONE shall maintain such designated list in electronic form.

Further a check will be run on regular basis to verify whether individuals or entities listed in the order are invested in the AIF schemes;

c) In the event any customers match the particulars of designated individuals / entities shall not later than 24 hours from the time of finding out such customer inform full particulars of such investments 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 on post shall also be sent through email at jsis@nic.in.

d) 360 ONE shall send particulars of the communication stated above through (i) 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 (East), Mumbai – 400 051 as well as the UAPA nodal officer of the state / UT where the account is held, and to FIU-IND.

e) In case the aforementioned details of any of the customers match the particulars of designated individuals / entities beyond doubt, IIFL AMC shall block such folios and prevent 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 on post shall also be sent through email at jsis@nic.in.

f) 360 ONE shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts.

In case of unfreezing and erroneous freezing of account the procedure laid down in the SEBI AML (Master circular) shall be followed. Specific to information request received from Nodal officer at SEBI pursuant to request made by other countries under U.N. Security Council Resolution 1373, the process entailed hereabove and under SEBI AML (Master Circular) shall be followed.

**O. Others**

This Policy is to be made available to the persons engaged in the depository operations for compliance purpose

Clients are to be categorized into low, medium and high risk based on perceived risk depending upon client's background, type of business activity, transaction etc. The Company shall put in place a system of periodical review of risk categorization of accounts, with such periodicity being at least once in 2 Years and the need for applying enhanced due diligence measures

The periodicity of updating of documents taken during the client due diligence (CDD) process will be every year

This PMLA policy will be reviewed yearly basis and or based on circulars issued by statutory authority from time to time and this updated policy should be approved in the meeting of Board of Directors.

All the clauses of this PMLA Policy should be reviewed periodically. Review of policy is to be done by any official other than the official who originally drafted the policy

In the case of any further information /clarification is required in this regard, the "Principal Officer" may be contacted for any information or clarification on the company's Anti Money Laundering Policies, contact / write to the following address:

The Principal Officer / Designated Director shall submit Suspicious Transactions Report (STR) and Cash Transaction Report (CTR) within the time frame prescribed under the Rules, to the Director, Financial Intelligence Unit (FIU), India in manual and electronic format.

No restrictions shall be placed on clients whose transactions have been reported to FIU – IND.

No tipping off to the client should be done at any level.

Irrespective of the amount of transaction and / or the threshold limit envisaged for predicate offences, reporting shall be done if the Principal officer believes that the transaction involves proceeds of crime.

**360 ONE WAM Limited**
**Legal & Compliance Dept.**
360 ONE Centre, Kamala Mills Compound,
Senapati Bapat Marg,
Lower Parel,
Mumbai – 400 013
Ph- 022 39585717
Email: brokingcompliance@iiflw.com