ISFL Handbook On

Anti-Money Laundering and Terrorist Financing

Contents

1. Introduction

M/s. Indsec Securities and Finance Limited (hereinafter called as "ISFL"), is a company incorporated under the Companies Act, 1956 and having its registered office at 301/302, "215 Atrium", A Wing, Andheri Kurla Road, Chakala, Andheri (East), Mumbai – 400 093. ISFL being an intermediary registered under section 12 of the SEBI Act 1992 (as a registered Stock Broker, Trading and Self Clearing Member, Depository Participant, Portfolio Manager) is committed to full compliance of India's Prevention of Money Laundering Act, 2002 (PMLA) and taking appropriate steps to prevent, detect and report the possible misuse of ISFL's products and services for money laundering activities.

To ensure compliance with the AML Laws, ISFL has adopted this Handbook which sets out procedures in relation to money laundering prevention and detection measures, which are based on the following:

a. India's Prevention of Money Laundering Act, 2002 (PMLA), as amended and Rules notified there under;
b. Securities and Exchange Board of India's (SEBI) Guidelines on Anti Money Laundering Standards – issued from time to time;
c. Securities and Exchange Board of India (Prohibition of Insider Trading) Regulations, 2015 (as revised from time to time).

This Handbook is to be used for all processing all the activities of ISFL as the Stock Broker, Depository Participant, Portfolio Manager.

2. Definition of Money Laundering & Terrorist Financing

Money Laundering can be defined as the process by which persons attempt to hide and disguise the true origin and ownership of the proceeds of corruption, bribery and fraud. Terrorist Financing can be defined as the process by which funds are collected with the intention or knowledge to use them to carry out the unlawful use of force against people or property. Both these issues continue to be of serious concern worldwide and have a multitude of wide ranging impacts on the reputations of countries, cultures and economies.

Financial institutions (including SEBI registered intermediaries) are attractive to money launderers and persons wishing to finance terrorism, as the services they offer can be used to help conceal the true origins of the monies. As a result, all financial firms and their employees have a legal and moral responsibility to help combat money laundering and the financing of terrorism. Financial institutions must also ensure that preventative measures are in place to help deter such activity.

The process of money laundering normally goes through three stages:

- **Placement** – the purchase of assets / shares / investments using the 'dirty' money, perhaps mixed in with 'clean' money;
- **Layering** – the movement of the money between different financial investments / institutions to confuse the trail for the authorities; and
- **Integration** – the movement of the money into e.g. another economy or business venture giving the money the appearance that it is legitimate.

3. Roles & Responsibilities

3.1 AML Committee

The AML Committee comprising of the Managing Director and Principal Officer (PO). Managing Director has been entrusted with the following responsibilities:

- To consider internal suspicious transaction reports
- To discuss and make decisions on policy matters, including but not limited to classification of customers as per risk profile.
- To guide the PO on any matter in relation to or connected with AML Laws and this Handbook, and to review this Handbook as and when revised/amended by PO, in order to comply with regulatory updates
- To determine transactions to be reported on recommendations from the PO

3.2 Principal Officer

Mr. Yogesh Kokatay, Vice President is appointed as the AML Principal Officer (PO). The PO is responsible for:

- Monitoring compliance with AML Laws and this Handbook.
- Revising this Handbook as and when necessary:
  - To ensure that all current requirements of the AML Laws are reflected and addressed, and
  - To ensure that this Handbook continues to represent adequate and appropriate management controls to achieve ongoing compliance with the AML Laws.
- Overseeing and coordinating external reporting of suspicious activities, and all other required reporting, to the applicable governmental authorities.
- Responding promptly to any reasonable request for information made by government officials.
- Supervising an ongoing employee AML training program
- Serving as a member of the AML Committee with responsibility for overseeing the efforts of the committee members with respect to their responsibilities related to ISFL's compliance with this Handbook and the AML Laws.
- Ensuring periodic testing of ISFL's compliance with this Handbook and the AML Laws by internal auditors.

3.3 Designated Director

- Mr. Diamond Dand, Whole-time Director of the Company is appointed as the Designated Director.
- The Designated Director shall observe the procedure and the manner of furnishing information as specified by SEBI from time to time and shall ensure overall compliance with the AML Laws and this Handbook.

3.4 Heads of Division / Departments

- Heads of Divisions / Departments have the following responsibilities:
- Implementation of ISFL's AML program in accordance with this Handbook within their respective domain and ensuring compliance by their staff.
- Ensuring the proper maintenance of all records with regards to transactions under their purview.
- Developing and customizing their respective operational procedures in conjunction with

this Handbook.

- Ensure all staff under their reporting authority undergo AML and suspicious transaction reporting training and are aware of the reporting formalities and the reporting lines clearly and that they have access to information, policy, report formats and relevant manuals.

3.5 All Staff

All Staff in ISFL (Involved in Dealing, Depository, Backoffice, Accounts & Compliance) have the following responsibilities:

- To be vigilant and aware of the guidelines provided in this Handbook.
- To be vigilant in detecting and reporting all suspicious transactions to their supervisor or the PO.
- Maintain utmost confidentiality on accounts identified as suspicious and not to discuss their suspicions with anyone except their supervisor and/or the PO.
- Understand the reporting formats and the reporting lines clearly.
- Undergo training on AML and suspicious transaction reporting procedures.

4. Client Due Diligence (CDD)

- Client Identification Procedures shall be carried out at the different stages i.e.;
  a. While establishing the relationship with the client
  b. While carrying out transactions on client's behalf
  c. When ISFL has doubts regarding previously obtained data

- The following CDD measures, as applicable, shall be applied to all the clients:
  - Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using client identification and verification procedures.

  - Verify the client's identity using reliable, independent source documents, data or information; Where the client purports to act on behalf of juridical person or individual or trust, the ISFL shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

  - Identify beneficial ownership and control of the client. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement. The beneficial owner 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: -
    i. "Controlling ownership interest" means ownership of or entitlement to more than ten per cent of shares or capital or profits of the company;

ii. "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 ten percent of capital or profits of the partnership or who exercises control through other means.

Explanation: - For the purpose of this clause: -
"Control" shall include the right to control the management or policy decision;

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 ten 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.

- Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to III;

- Understand the ownership and control structure of the client;

- Conduct ongoing due diligence and scrutiny, i.e. Perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the ISFL's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds;

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

- ISFL shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process such that the information or data collected under client due diligence is kept up-to-date and relevant, particularly for high risk clients.

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

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

- No transaction or account-based relationship shall be undertaken without following the CDD procedure.

- **Client Identification Procedures and Policy for acceptance of clients**

  New customer acceptance procedures, inter alia, includes following processes

  - Individual clients:
    - PAN Verification
    - In Person Verification
    - Verification of documents with Originals
    - Obtaining Bank statements / IT returns to ascertain risk categorization Obtain and Verify Aadhar

  - **Non-Individual Clients:**
    - PAN Verification
    - Verification of documents with Originals Accessing financial results
    - Establishing the identity of Ultimate Beneficiary Obtain and Verify Aadhar of Authorised Signatory

  Clients of special category shall be classified as high-risk clients. Enhanced due diligence measures shall be applicable for Clients of Special Category (CSC) as given below:

  a. Non-resident clients
  b. High net worth clients,
  c. Trust, Charities, NGOs and organizations receiving donations
  d. Companies having close family shareholdings or beneficial ownership
  e. Politically Exposed Persons" (PEPs).
  f. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent.
  g. Non face to face clients
  h. Clients with dubious reputation as per public information available etc.

  The above-mentioned list is only illustrative and the staff should exercise independent judgment to ascertain whether new clients should be classified as CSC or not.

  Senior Management approval should be obtained in case the client is identified as a PEP, whether while account opening or subsequently. Sources of funds and Beneficial Ownership needs to be identified in case of PEP clients.

- The client identification must be done by using resources such as PAN database website, Ministry of Corporate Affairs website and such other authentic sources.

- The Aadhar of the client (in case of Individual Client) or of the Authorized Signatory of the client (in case of Non-Individual client) shall be obtained within a stipulated period. In case the client/authorized signatory is not eligible to obtain Aadhar, a copy of PAN or form 60 as defined in Income-tax Rules, 1962 shall be obtained. Further, incase client/authorized signatory is exempted from obtaining PAN, a copy of officially valid document shall be obtained.

- The information obtained must be adequate to satisfy the regulators and enforcement agencies that the Client due diligence was in compliance with the specified guidelines. Failure to provide the requested information by client should be reported to higher authorities immediately.

- ISFL to ensure that account is not opened in benami/fictitious/anonymous name or in case the above mentioned CDD measures/policies could not be satisfied fully. This is applicable in cases where the identity of client or the information obtained is suspect or the client is perceived to be non-cooperative.

- No exemption is provided from carrying out Client Due Diligence in respect of any category of clients within PML, thus irrespective of low volume of trade etc, the mandated information should be obtained from all active clients.
    - To cover proposed customer identification and verification depending on nature /status of the customer and kind of transactions that are expected by the customer.
    - To comply with guidelines issued by various regulators such as SEBI, RBI etc.
    - To clearly establish identity of the proposed client, verification of addresses, phone numbers and other details.
    - To obtain sufficient information in order to identify persons who beneficially own or control the trading account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by entity other than the client.

- Following procedure is specified to allow another person/entity to act on behalf of client:
    - Letter signed by client clearly mentioning the name of the person, his contact number and his email id should be obtained.
    - In case of the corporate bodies the board resolution obtained should clearly name the persons authorized to act of behalf of the entity. A letter specifying the names of authorized persons, email ids, contact numbers should be obtained in such cases.

- Apart from the mandatory information specified by SEBI, additional information as deemed fit on case to case basis to satisfy themselves about the genuineness and financial standing of the proposed client is being asked for, including following:
    - To check whether the client has any criminal background, whether he has been at any point of time been associated in any civil or criminal proceedings anywhere.
    - To check whether at any point of time he has been banned from trading in the stock market.
    - To check if the proposed client's name appears in the List of Designated Individuals / Entities as detailed in Para 10 of this handbook.
    - To ensure that an account is not opened if any of the information collected is adverse.
    - To ensure authenticity of a person's authority to act on behalf of the client. This should be an ongoing exercise periodically while carrying out client transactions.

- Risk based KYC procedures should be adopted for all new clients. Reluctance on the part of the client to provide necessary information or cooperate in verification process could generate a red flag for the member for additional monitoring.

- The information obtained through the above-mentioned measures should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the Guidelines.

- For existing clients processes includes,
    - Review of KYC details of all the existing active clients in context to the PMLA ACT requirements.
    - Classification of clients into high, medium or low risk categories based on KYC details, trading activity etc for closer monitoring of high risk categories etc.

    - Obtaining of annual financial statements from all clients, particularly those in high risk categories.
    - In case of non individuals additional information about the directors, partners, dominant promoters, major shareholders to be obtained to identify the ultimate beneficial owner.
    - Perform ongoing scrutiny of transactions and account to ensure that the transactions are consistent with the financial information available with ISFL based on the risk profile.
    - Updation of documents or data with respect to all active clients and ultimate beneficial owners like financial results, Aadhar of the client (in case of Individual Client) or of the Authorized Signatory of the client (in case of Non-Individual client). (In case the client/authorized signatory is not eligible to obtain Aadhar, a copy of PAN or form 60 as defined in Income-tax Rules, 1962 shall be obtained. Further, incase client/authorized signatory is exempted from obtaining PAN, a copy of officially valid document shall be obtained.)

- Obtain additional information, declaration from clients with respect to high value transactions, wherever deemed fit.

- To ensure that if any of the above information obtained from the clients is adverse, his business is immediately suspended and respective account be frozen or closed. Further ISFL in consultation with relevant exchange or depository may decide course of further action with regards to the funds and securities in ISFL's custody if any. Any amount collected under this clause shall be remitted to the SEBI for credit to the Investor Protection and Education Fund administered by the Board under the Act."

- To continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list of designated Individuals/Entities as stipulated in Para 10 of this handbook

5. Reliance on Identification Already Performed

- ISFL may rely on a third party for the purpose of –
    - identification and verification of the identity of a client and
    - Determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner.
    - Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act.

- Such reliance shall be subject to the following conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time:
    - ISFL shall immediately obtain necessary information of such client due diligence carried out by the third party;
    - ISFL shall take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay.
    - ISFL shall satisfy itself 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;
    - The third party is not based in a country or jurisdiction assessed as high risk;

- ISFL must establish a contractual agreement with the third party to cover the adherence of AML Laws relating to verification of the customer's identity and address.

6. Risk Management

- **Risk-based Approach:**
  It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. Accordingly, Risk categorization of both the new and existing clients shall be done into high, medium or low risk category depending on parameters such as the customer's background, type of business relationship, transactions etc. on a case to case basis. The customer due diligence measures can be applied to each of the clients based on their risk category where an enhanced customer due diligence process may be adopted for high risk categories of clients and vice-á-versa.

- **Risk Assessment:**
  Risk assessment shall be done to identify, assess and take effective measures to mitigate the money laundering and terrorist financing risk with respect to the clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc.

All the relevant risk factors shall be considered before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

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.

7. Monitoring of Transactions

Ongoing monitoring of accounts is an essential element of an effective Anti Money Laundering framework. Such monitoring should result in identification and detection of apparently abnormal transactions, based on laid down parameters. ISFL should devise and generate necessary reports/alerts based on the clients' profile, nature of business, trading pattern of clients for identifying and detecting such transactions. These reports/alerts should be analyzed to establish suspicion or otherwise for the purpose of reporting such transactions.

A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:

- Clients whose identity verification seems difficult or clients appear not to cooperate
- Substantial increase in activity without any apparent cause
- Large number of accounts having common parameters such as common partners / directors / promoters / address / email address / telephone numbers / introducers or authorized signatories;
- Transactions with no apparent economic or business rationale
- Sudden activity in dormant accounts;
- Source of funds are doubtful or inconsistency in payment pattern;
- Unusual and large cash deposits made by an individual or business;
- Transfer of investment proceeds to apparently unrelated third parties;
- Multiple transactions of value just below the threshold limit specified in PMLA so as to avoid possible reporting;
- Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export- import of small items.;
- Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
- Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
- Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
- Purchases made on own account transferred to a third party through off market transactions through DP Accounts;
- Suspicious off market transactions;
- Large deals at prices away from the market.
- 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.
- Trading activity in accounts of high risk clients based on their profile, business pattern and industry segment.

8. Suspicious Transactions

- **Definition of a suspicious transaction**
  The Rules notified under the PMLA defines a "suspicious transaction" as a transaction whether or not made in cash which, to a person acting in good faith:
  - Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime
  - Appears to be made in circumstances of unusual or unjustified complexity
  - Appears to have no economic rationale or bonafide purpose.
  - Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

- **Definition of "Transaction at Risk"**
  "Transaction at Risk" is the term used internally within ISFL to designate a transaction that may indicate a suspicious transaction but given the need for additional information, is not yet deemed a "suspicious transaction."

  The reason we distinguish between "suspicious transactions" and "Transactions at Risk" is to ensure that we are clear and precise in all internal communications.

  Please note that the examples listed below could also be easily resolved by following the appropriate procedures, and thus are not necessarily suspicious in their own right.
  - Application received from a potential shareholder resident in a NCCT country
  - Third party incoming payment
  - A shareholder who has invested minimal amounts every year for the past two years, and starts investing huge amounts on a month to month basis.

  Transactions deemed to be at risk should be documented on the "Transactions at Risk form."

  In addition to the automated monitoring system, wherever applicable, all staff who have a suspicion of money laundering activity on any accounts or any transactions, regardless of amount, shall promptly report the transaction to their immediate superior or the PO.

  Any doubts about a transaction should be discussed immediately with their immediate superior / or the PO.

- **Reporting Procedure**

  Step – 1
  Responsibility: Trade Control Team
  - Generate periodic System reports for transactions at risk which will be done by Trade Control Team

  Responsibility: All Staff
  - Report to your Supervisor, Transactions at Risk using standard format as specified.
  - Maintain utmost confidentiality and do not discuss your suspicions with anyone other than their Supervisor and/or PO
  - Supervisor will review the reports and forward the same to the PO (where the report is submitted directly to PO – go straight to Step 3)

  Failure on the part of staff to report any such transaction may subject the concerned staff to disciplinary action.

Step – 2
Responsibility: Trade Control Team

- Review the System reports and internal reports from staff
- Investigate them by going through the transactions of the customer across accounts
- Take feedback from Sales and Branch staff , if required
- Send Report to the PO on trades identified as suspicious
- Generate necessary reports in the required formats

Step -3
Responsibility – PO

- Review the transaction at risk with the ISFL AML Committee
- Where decision has been made to file US, filing must be done within 7 days of arriving at the decision.

Responsibility – Designated Director

- Review and supervise the process of reporting the suspicious transactions to PO and ensure effective compliance of the guidelines stipulated by SEBI from time to time.

- **The STRs are to be filed at the following address:**
  Director, FIU-IND
  Financial Intelligence Unit - India
  6th Floor, Tower-2, Jeevan Bharati Building
  Connaught Place, New Delhi-110001, INDIA
  Telephone: 91-11-23314429, 23314459
  91-11-23319793(Helpdesk) Email: helpdesk@fiuindia.gov.in

  Website: **http://fiuindia.gov.in**

No restrictions shall be put on operations in the accounts where an STR has been filed. ISFL, its directors and employees shall not disclose any information about the filed STR to be client.

Irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, ISFL shall file STR if it has reasonable grounds to believe that the transactions involve proceeds of crime.

"Proceeds of crime" include property not only derived or obtained from the scheduled offence but also any property which may directly or indirectly be derived or obtained as a result of any criminal activity relatable to the scheduled offence.

Any change in the name of Principal Officer or the Designated Director has to be intimated to FIU immediately.

9. Internal Reporting for Transaction at Risk

Processes for alert generation, examination and reporting could include(s) -

- Audit trail for all alerts generated till they are reported / closed
- Clear enunciation of responsibilities at each stage of process from generation, examination, recording and reporting
- Escalation through the organization to the principal officer designated for PMLA
- Confidentiality of STRs filed

- Retention of records for a period of 5 years
- If the nature of suspicious trading cannot be categorized by any of the preset risk categories, please describe the nature of the suspicion as best as possible under "Others". Please include all information which you think may be helpful in assisting in their investigations. Examples of these are:
    - What aroused the staff's suspicion (i.e. deviation from the standard operation of the account, forgery of documents etc.)? State the actual reason for the suspicion
    - The date of any meetings which the staff may have with the Customer
    - What was discussed?
    - What transaction(s) did the customer want to undertake?
    - Why did the customer want to undertake the transaction(s)?
    - What questions did the staff ask the customer in relation to the transaction?
    - What was the customer's response?
    - Did the customer display any emotion e.g. was the customer agitated, evasive etc?
    - Did the staff ask any further questions and what was the Customer's response?
- All reports must be sent via their supervisors who also ensure that the report is properly and accurately filled up before it is sent to the PO.
- The relevant documents that should accompany the internal report for "Transaction at Risk" are as follows:
    - All account opening forms.
    - All customer identification documents, if any.
    - Recent account history including copies of the computer printout from the system.
    - Documents evidencing the suspicious transaction(s). This would include all relevant correspondences, invoices, agreements etc if any.
    - Other relevant documents such as company searches etc.

10. List of Designated Individuals/ Entities

- The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. ISFL shall take note of such lists of designated individuals/terrorists, as and when communicated by SEBI.

- All orders under section 35 (1) and 51A of UAPA relating to funds, financial assets or economic resources or related services, circulated by SEBI from time to time shall be taken note of for compliance.

- An updated list of individuals and entities which are subject to various sanction measures such as freezing of assets/accounts, denial of financial services etc., as approved by the Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs) can be accessed at its website at **https://press.un.org/en/content/press-release**. The details of the lists are as under:

    - The "ISIL (Da'esh) &Al-Qaida Sanctions List", which includes names of individuals and entities associated with the Al-Qaida. The updated ISIL & Al-Qaida Sanctions List is available at: **https://www.un.org/securitycouncil/sanctions/1267/press-releases**.

    - The list issued by United Security Council Resolutions 1718 of designated Individuals and Entities linked to Democratic People's Republic of Korea **www.un.org/securitycouncil/sanctions/1718/press-releases**.

- ISFL shall ensure that accounts are not opened in the name of anyone whose name appears in said list. ISFL shall continuously scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.

- ISFL shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions carried through or attempted in the accounts covered under the list of designated individuals/entities under Section 35 (1) and 51A of UAPA.

- Full details of accounts bearing resemblance with any of the individuals/entities in the list shall immediately be intimated to the Central [designated] Nodal Officer for the UAPA, at Fax No. 011-23092551 and also conveyed over telephone No. 011-23092548. The particulars apart from being sent by post shall necessarily be conveyed on email id: **jsctcr-mha@gov.in**.

- ISFL shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND, without delay. The communication shall be sent to SEBI through post and through email (sebi_uapa@sebi.gov.in) to the UAPA nodal officer of SEBI, Deputy General Manager, Division of FATF, Market Intermediaries Regulation and Supervision Department, Securities and Exchange Board of India, SEBI Bhavan II, Plot No. C7, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051. The consolidated list of UAPA Nodal Officers is available at the website of Government of India, Ministry of Home Affairs.

11. Record Keeping & Retention

Compliance should be ensured with respect to record keeping as specified under the SEBI Act 1992, Rules and Regulations made there under, PMLA as well as other relevant legislation, rules, Regulations, Exchange Bye-laws and Circulars.

All records for both domestic as well as international clients shall be stored securely in a manner that allows for easy retrieval and should at a minimum contain the following:

ISFL shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities whenever sought. To enable this, following information shall be retained for all the clients:

i. the beneficial owner of the account;
ii. the volume of the funds flowing through the account; and
iii. for selected suspicious transactions:
    a. the origin of the funds
    b. the form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
    c. the identity of the person undertaking the transaction;
    d. the destination of the funds;
    e. the form of instruction and authority.

ISFL shall maintain proper record of transactions prescribed under Rule 3 of PML Rules as mentioned below:

i. all cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency;

ii. 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;
iii. 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;
iv. all suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into or from any non-monetary account such as demat account, security account maintained by the registered intermediary.

Following information shall be maintained and preserved in respect of transactions referred to in Rule 3 of PML Rules:

- the nature of transaction;
- the amount of the transaction and the currency in which it was denominated;
- the date on which the transaction was conducted; and
- the parties to the transaction.

Records shall be maintained properly and preserved in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities. Further, the records mentioned in Rule 3 of PML Rules have to be maintained and preserved for a period of five years from the date of transactions. Records evidencing the identity of clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of five years after the business relationship between a client and ISFL has ended or the account has been closed, whichever is later. In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed. The records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND, as required under Rules 7 and 8 of the PML Rules, shall be maintained and preserved for a period of five years from the date of the transaction.

Irrespective of the retention period, records of the Customers shall not be destroyed without the prior consent of the PO.

12. Employees Hiring and Training

ISFL shall develop adequate screening procedures and high standards while hiring employees, so that employees taking up key positions are suitable and competent to perform their duties in view of the risk of money laundering and terrorist financing.

ISFL has taken appropriate measures so that all staff is aware of their responsibilities and ISFL's approach to deter money-laundering and the financing of terrorism. These measures are:

- Every new staff must attend anti-money laundering training presentation, if any
- Every time the AML Handbook is updated, staff shall be informed of the update.
- Departmental Managers shall be responsible for ensuring that their staff do attend the anti-money laundering training sessions and for identifying any potential training needs.
- Specific briefings shall be provided to all staff from time to time, as appropriate, on particular issues relating to money laundering and the financing of terrorism.

13. Periodic Review of Policy

This policy shall be reviewed annually by the Board of Directors. The changes required to be made in the policy, if any, pursuant to the amendments in the applicable laws and regulations shall be made forthwith and the amended policy shall be placed before the Board for its approval.

14. Investor Education and Awareness

The policy shall be communicated to the clients at the time of account opening and also placed on the website of the company. Suitable measures shall be taken to create awareness on the objectives and requirements of the AML/CFT framework.

15. Audit

ISFL's Internal Auditors shall periodically audit and test ISFL compliance with this Handbook and the policies, procedures, and controls relating to the prevention of Money Laundering and Terrorist Financing.

Findings of the Internal Audit shall be reported to the Board for further actions required to be taken, if any, including amendments to the policies and procedures.

----------×----------×----------