“ISFL” Handbook On

Anti-Money Laundering and Terrorist Financing

Table of 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 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 on January 18, 2006 and March 20, 2006

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. Nandkishore Gupta, Managing 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. General Client Due Diligence

Different stages at which the KYC policy is applicable

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

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

- 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.

No exemption is provided from carrying our 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, members should ask for any additional information as deemed fit on case to case basis to satisfy themselves about the genuineness and financial standing of the proposed client, 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 www.watchoutinvestors.com and http://www.un.org/sc/committees/1267/consolist.shtml (list of designated individuals/ entities published by United Nations Security Council). Ensure that account is not opened if the name is appearing in any of the above lists.

    - To ensure that an account is not opened where ISFL is not able to obtain any other above information or any of the information collected in 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.

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

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.

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.

- 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 by United Nations Security Council Committee published at http://www.un.org/sc/committees/1267/consolist.shtml

- Section 51A, of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities, empowers the Central Government to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism. Therefore, ISFL shall ensure swift implementation of any order under Section 51 A of UAPA received from Government Agencies to freeze, seize or attach funds and other financial assets held by, on behalf of the notified individual / entity.

- In addition to the above ISFL shall monitor the clients on Countries or geographical locations, specifically 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 Security Council Resolutions which can be accessed at :
  http://www.un.org/sc/committees/1267/aq_sactions_list.shmtl
  and
  http://www.un.org/sc/committees/1988/list.shtml

Risk based approach:

Classify both the new and existing clients into high, medium or low risk category depending on parameters such as the customer's background, type of business relationship, transactions etc. Members should apply each of the customer due diligence measures on a risk sensitive basis and adopt an enhanced customer due diligence process for high risk categories of customers and vice-á-versa.

Clients of special category (CSC)

Such clients include the following

- Non resident clients
- High net worth clients,
- Trust, Charities, NGOs and organizations receiving donations
- Companies having close family shareholdings or beneficial ownership
- Politically exposed persons (PEP) of foreign origin
- Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
- Companies offering foreign exchange offerings
- 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.
- Non face to face clients
- Clients with dubious reputation as per public information available etc.

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

5. Reliance on Identification Already Performed

When reliance is being placed on any third party to identify or confirm the identity of any customer, 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.

Where the third party is a channel partner, certification from the channel partner is to be obtained stating fulfillment of the AML Laws on an annual basis.

6. Suspicious Transactions

6.1 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.

6.2 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.

6.3 Ongoing monitoring of accounts

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. Members should devise and generate necessary reports/alerts based on their 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 transaction**s.**

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.

6.4 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 STR, 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, Hotel Samrat, Chanakyapuri,
New Delhi – 110021
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.

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

7. Internal Reporting for Transaction at Risk

Processes for alert generation, examination and reporting could include

- 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.

8. Record Keeping & Retention

Records confirming the identity of Client and the Customer transactions shall be retained for a minimum period of **five years** following the cessation of the business relationship or closure of account 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 beyond a period of five years until it is confirmed that the case has been closed. Irrespective of the retention period, records of the Customers shall not be destroyed without the prior consent of the PO. Copies of STRs shall also be retained for a period of five years from the date of filing or till the date of closure of the concerned case, whichever is later.

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:

- 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.

ISFL shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities whenever sought.

ISFL shall maintain proper record of transactions prescribed under Rule 3 of PML Rules.

Viz : i) all transactions in foreign currency of/equivalent to value more than rupees ten lakhs.
ii) all integrally connected series of transactions in foreign currency totaling to more than ten lakhs.
iii) all suspicious transactions whether or not made in cash.

9. 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.

10. 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. The auditors also have access the awareness of front line staff.

The Internal Audit shall report all findings to the AML Committee.