

# **ABANS GROUP OF COMPANIES**

## **ANTI-MONEY LAUNDERING POLICY & PROCEDURES**

**(Revised Edition: Apr'2022)** updated 27.07.2022  
*[Board Resolutions Dated: ASPL / ABSPL / ACIPL - 18<sup>th</sup> Apr'22]*

## **INTRODUCTION**

Abans Group of companies is an active intermediary, participating in various arenas of Capital Market, Futures and Options, Currency Derivatives and Commodities Market Business which are carried through the various companies of the Group i.e.

1. Abans Securities Private Limited (ASPL).
2. Abans Broking Services Private Limited (ABSPL).
3. Abans Commodities (I) Private Limited (ACIPL).

Abans Group has always been at the forefront, towards ensuring compliance with all the regulatory requirements. As an effort in the same direction this policy statement has been prepared to ensure compliance under the Prevention of Money Laundering Act, 2002. This statement has been framed as a part of the overall procedures adopted by Abans Group of Companies to implement the Anti-money Laundering provisions envisaged under the PMLA, 2002.

This policy statement shall be applicable to all the Group Companies stated above.

### **1. Prevention of Money Laundering Act, 2002**

The Prevention of Money Laundering Act, 2002 (PMLA 2002) forms the core of the legal framework put in place by India to combat money laundering. PMLA 2002 and the Rules notified there under came into force with effect from July 1, 2005. The Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections of the Act to implement the provisions of the Act.

The PMLA 2002 and rules notified there under impose obligation on all banking companies, financial institutions and intermediaries to verify identity of clients, maintain and review records, monitor transactions with clients, and furnish information to FIU-IND. PMLA 2002 defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime.

Extract of Obligations imposed on Intermediaries under PMLA 2002, clause 12:

(12) (1) Every banking company, financial institution and intermediary shall-

- (a) Maintain a record of all transactions, the nature and value of which may be prescribed, whether such transactions comprise of a single transaction or a series of transactions integrally connected to each other, and where such series of transactions take place within a month;
- (b) Furnish information of transactions referred to in clause (a) to the Director within such time as may be prescribed;
- (c) Verify and maintain the records of the identity of all its clients, in such a manner as may be prescribed.

Provided that where the Principal Officer of a Banking Company or Financial Institution or Intermediary, as the case may be has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed limit so as to defeat the provisions of this section, such officer shall furnish information in respect of such transactions to the Director within the prescribed time.

(2) the records referred to in sub-section (1) shall be maintained for a period of Five years from the date of cessation of the transactions between the clients and the banking company or financial institute or intermediary, as the case may be.”

## **2. Applicability and Scope of PMLA 2002**

Subsequent to the PMLA 2002, coming into force with effect from 1st July 2005, SEBI issued necessary guidelines vide updated master circular on AML/CFT no. CIR/ISD/AML/3/2010 dated 31.12.2010 and subsequently superseding it vide SEBI Master Circular no. SEBI/HO/MIRSD/DOS3/CIR/P/2018/104 dated 04.07.2018 replaced by **SEBI Master Circular no. SEBI/HO/MIRSD/DOP/CIR/P/2019/113 dated 15.10.2019** to all securities market intermediaries registered under Section 12 of the SEBI Act, 1992. These Guidelines lay down the minimum requirements / disclosures to be made in respect of clients. However, intermediaries may, based on their internal risk management, specify additional disclosures to be made by clients to address concerns of Money Laundering and suspicious transactions undertaken by clients.

The said circular issues guidelines to be followed by all Stock brokers, Sub brokers and Depository Participants. Section 1 of the circular gives an overview of the obligations to be followed.

### **The obligations imposed are as under:**

1. Each registered intermediary should issue a statement of policies and procedures on a group basis where applicable for dealing with Money Laundering and Terrorist Financing reflecting the current statutory and regulatory requirements
2. Adopt client acceptance policies and procedures and undertake client due diligence measures which are sensitive to the risk of Money Laundering and Terrorist Financing, and have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.
3. Ensure that the content of these Guidelines is understood by their staff members and develop staff members’ awareness and vigilance to guard against Money Laundering and Terrorist Financing
4. Should regularly review the policies and procedures on prevention of money laundering and terrorist financing to ensure their effectiveness. Further in order to ensure effectiveness of policies and procedures, the person doing such a review should be different from the one who has framed such policies and procedures;

**SEBI primarily vide its master circular no CIR/ISD/AML/3/2010 dated 31.12.2010 – Part II had given detailed directives vide points 4 to 15 therein for implementation by the intermediaries.**

**Further there were other regulatory circulars that are taken into consideration for preparation of this policy. Various directives and Abans initiatives in compliance of the same are given below:**

1. CIR/MIRSD/1/2014 dt. 12.3.2014 - AML/CFT Obligations of securities market intermediaries under PMLA - 2002
2. ISD/AML/CIR-2/2009 dt. 23.10.2009 – Combating Financing of Terrorism under Unlawful Activities (Prevention) Act 1967 (UAPA)
3. CIR/MIRSD/2/2013 dt. 21.1.2013 – Guidelines regarding identification of Beneficial Ownership
4. F. NO9-6/AG-II/2012/ FIU-IND dt. 11.3.2016 – Guidelines for detecting suspicious transactions under PMLA 2005

Finally on 4<sup>th</sup> July, 2018, SEBI vide its Master Circular no SEBI/ HO/ MIRSD/ DOS3/ CIR/ P/ 2018/ 104 dated 04.07.2018 – Part II superseding the earlier Master Circular on AML / CFT dated 31<sup>st</sup> Dec, 2010 replaced by SEBI Master Circular no. **SEBI/HO/MIRSD/DOP/CIR/P/2019/113 dated 15.10.2019** has given detailed directives and guidelines on Anti-Money Laundering (AML) Standards and Combating the Financing of Terrorism (CFT) /Obligations of Securities Market Intermediaries under the Prevention of Money Laundering Act, 2002 and Rules framed there under, for implementation by the intermediaries to ensure compliance with AML / CFT directives.

**FIU India, in addition, issued Supplemental Guidelines on Red Flag Indicators (RFIs) vide F. No. 9-2/2021/Intermediaries/FIU-IND dated July 21, 2022.**

### **3. Written Anti Money Laundering Procedures (Point -4 (Point 2.1 of the Latest Circular))**

Each registered intermediary shall adopt written procedures to implement the Anti-Money Laundering provisions as envisaged under the PMLA. Such procedures shall include inter alia, the following three specific parameters which are related to the overall „Client Due Diligence Process

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

#### **Abans Initiative:**

Abans has prepared the policy statement covering all the points as per the guidelines to ensure compliance under the Prevention of Money Laundering Act, 2002. This statement has been framed as a part of the overall procedures adopted by Abans Group of Companies to implement the Anti-money Laundering provisions envisaged under the PMLA, 2002. This policy statement shall be applicable to all the Group Companies, including all the branches and regional offices.

The policy has been approved by the Board in its meeting held on June 18, 2014 and the subsequent modifications as per fresh SEBI guidelines also approved by the Board in its meeting held on March 21, 2017. The policy shall be reviewed annually and updated periodically as and when fresh/ revised guidelines are issued by the regulators, with proper version controls, and shall be placed before the Board for approval.

### **4. Customer Due Diligence Process (Point 5 (Point 2.2 of the Latest Circular))**

The Company shall put in place appropriate customer due diligence measures, which should be applied to all customers (new as well as existing). These measures comprise,

- 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 should be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

- Verify the client's identity using reliable, independent source documents, data or information;
- Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted;
- Verify the identity of the beneficial owner of the client and/or the person on whose behalf a transaction is being conducted corroborating the information provided in relation to (c);
- 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 registered intermediary's knowledge of the client, its business and risk profile, taking into account, where necessary, the client's source of funds.
- Registered Intermediaries shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process
- All registered intermediaries are required to obtain senior management approval for establishing business relationships with Politically Exposed Persons (PEPs)

**(a) Procedure for Identification and Verification of Customers:**

- i. Before admitting any person as a customer, the Company shall obtain sufficient information in order to identify the customer and any other person(s) with whom lies the beneficial ownership or ultimate control. The same should be done for all the existing customers as well. This should be done by obtaining "Know Your Customer" (KYC) information.
- ii. KYC information should be updated on a regular basis during the course of business relationship.
- iii. The customer should be identified by the Company using documents/information from reliable sources. Adequate information to satisfactorily establish the identity of each client and the purpose of the intended nature of the relationship should be obtained by the Company.
- iv. The procedure to be followed for admitting a person as a client is as under:
  - (i) Client/Client's Nominee/Company's Sales Executive should submit the account opening form/client registration form duly filled-in and signed by the prospective client.
  - (ii) The Client should provide all the necessary information required along with the relevant documents. Following documents should be collected from non-individuals' clients:
    1. Non-individual Client Registration Form;
    2. Rights and obligations;
    3. Risk Disclosure Document;
    4. Policies and Procedures
    5. Guidance Note (Do's and Don'ts)

6. Tariff sheet
7. All other supporting documents for identity/address of the non-individual entity and the authorized signatory;
8. In case of companies, board resolution authorizing the directors/senior employees/ authorized signatory to operate on behalf of the company and to deal in the derivative market. In case of other entities, similar documents would be required;
9. PAN Card copy of Non-individual client and all the partners/directors in case the client is a partnership firm or body corporate;
10. Bank Account proof.

- Following documents are to be collected from individual clients:

1. Individual Client Registration Form;
2. Rights and obligations;
3. Risk Disclosure Document;
4. Policies and Procedures
5. Guidance Note (Do's and Don'ts)
6. Tariff sheet
7. All other supporting documents for identity and residence of the individual;
8. PAN Card copy;
9. Bank Account proof.

- Photo identity proof of client should be verified against originals. In case of a non-individual client, photo identities of the directors/authorized persons should be verified against originals and taken on record.

- If all the documents and form are in order, client should be allotted a Unique Client Code (UCC).
- Clients can start transacting only after they have been allotted UCC.

#### **(b) Policy for Acceptance of Clients**

The Company has developed customer acceptance policy and procedures which aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. Staff should adhere to following safeguards while accepting customers:

- No Trading account should be opened in a fictitious / benami name or on an anonymous basis, or in the name of a suspended/banned entity.
- No Trading account should be opened in the name of any person with criminal background.
- Members of the Company must not establish accounts or relationships involving unregulated money service businesses or unregulated businesses involved in gambling activities.
- No account should be opened if appropriate due diligence measures cannot be applied to a customer for want of verification of documents or on account of non-cooperation of the customer or due to non-reliability of the data/information furnished by the customer.

In case an account is being opened & operated by an agent on behalf of Principal, it should be specified in what manner the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further the rights and responsibilities of both the persons (i.e. the agent-client registered with Company).

#### **(c) Risk Profiling of Customers**

- (i) Risk profiling of all customers should be done based on factors such as customer background, location, nature of business activity or transaction, trading turnover etc. This should be done by the Account Opening Team in consultation with the Principal Officer of the Company. Based on the risk assessment,

customers should be grouped into the following three categories –

- 1. Low Risk**
- 2. Medium Risk**
- 3. High Risk**

- (ii) The Company shall apply customer due diligence measures to clients on a risk sensitive basis i.e. applicability of customer identification procedures, documentary requirements, ongoing account monitoring, transaction monitoring & risk management will depend on the risk profile of customer. Customers identified as high-risk category shall be subjected to enhanced customer due diligence process. Conversely, a simplified due diligence process may be adopted for low risk categories of customers.
- (iii) In certain limited circumstances, within the overall framework of the FMC guidelines, the Company may apply reduced or simplified Customer Due Diligence measures for certain types of customers, products or transactions, taking into account all the risk factors. Any such reduced customer due diligence procedures must be approved by the Principal Officer.
- (iv) Clients of Special Category (CSC): Customers who may pose a particular risk to the Company, to money laundering deterrence programme and to the Company's reputation, and who should normally be treated as high risk and subject to enhanced customer due diligence, include, but are not limited to the following:
- Offshore Trusts, Special purpose Vehicles, International Business Companies which are established in locations with strict bank secrecy or confidentiality rules, or other legislation that may impede the application of prudent money laundering controls
  - Private companies or public companies not subject to regulatory disclosure requirements and which are constituted in full or in part by bearer shares
  - Customers with complex account relationships e.g. multiple accounts in one
  - Non-Resident Clients
  - High Net-worth Clients
  - Trust, Charities, NGOs and organizations receiving donations
  - Companies having close family shareholdings or beneficial ownership
  - Politically Exposed Person (PEP): Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g. Heads of States or of Governments, senior politicians, senior government / judicial / military officers, senior executives of state-owned corporations, important political party officials etc. The norms applicable to PEP shall also be applied to the accounts of the family members or close relatives of PEPs
  - Companies offering foreign exchange offerings
  - Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect or which do not or insufficiently apply FATF standards, 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.

**Abans Initiative:**

In order to ensure that the guidelines are complied with, Abans group has implemented a Comprehensive System of Internal Control across the company. We have put in place a strict client profiling and monitoring system, encompassing client profiling at the account opening stage, critical examination of

trading pattern / holding pattern of the clients, demat transaction, periodical scrutiny of client account maintained with us and regular review of these policies and procedures.

The initiatives undertaken by our various departments, to implement AML/CFT (Anti money Laundering/Combating Financing of Terrorism) standards as envisaged under PMLA, 2002 and other regulatory authorities from time to time, are as under:

- The following safeguards are followed as a policy while accepting the clients-
- No account will be opened in a fictitious / benami name or on an anonymous basis.
- Mandatory SEBI guidelines such as in person verification, verification of PAN with Income-tax website, verification of original documents with the copies submitted shall be meticulously carried out with 100% verification by concurrent audit team.
- Ensuring that an account is not opened where it is not possible to ascertain the identity of the client, or the information provided is suspected to be non-genuine, or in case of non-co-operation of the client in providing full and complete information.
- Checks and controls before opening an account to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.
- Scanning of all existing accounts will be done to ensure that no account is held by or linked to any of the entities or individuals included in the 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) or any other banned or notified entity which can be accessed at <https://www.un.org/securitycouncil/ombudsperson> (for res. 1267); <https://www.un.org/securitycouncil/sanctions/delisting> (for other Committees); <https://www.un.org/securitycouncil/content/2231/list> (for res. 2231), While dealing with clients in those high risk countries where the existence/effectiveness of money laundering control is suspect, intermediaries apart from being guided by the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website ([www.fatf-gafi.org](http://www.fatf-gafi.org)), shall also independently access and consider other publicly available information.
- **We will strictly enforce any orders or notifications received from the Central Government to freeze, seize or attach funds and other financial assets or other economic resources held by, on behalf of, or at the directions of the entity listed in the schedule to the order, or any other person engaged in or suspected to be engaged in terrorism.**
- **We will also ensure strict adherence to any government order or notification prohibiting any individual or entity from making any funds, financial assets or economic resources or related services available for the benefits of the individuals or entities listed in schedule to the order or any other person engaged in or suspected to be engaged in terrorism.**
- In the event, particulars of any of customer/s match the particulars of designated individuals/entities, we shall immediately, **not later than 24 hours from the time of finding out such customer**, inform full particulars of the funds, financial assets or economic resources or related services held in the form of securities, held by such customer on our books to **the Joint Secretary (IS.I), Ministry of Home Affairs**, at **Fax No.011-23092569** and also convey over telephone on **011-23092736**, besides conveying through e-mail at [jisis@nic.in](mailto:jisis@nic.in). Further we shall also intimate the particulars through **post/fax** and through **e-mail ([sebi\\_uapa@sebi.gov.in](mailto:sebi_uapa@sebi.gov.in))** to the UAPA nodal officer of SEBI, **Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan, Plot No. C4-A, "G" Block, Bandra Kurla Complex, Bandra (E), Mumbai 400 051** as well as the UAPA nodal officer of the state/UT where the account is held, as the case may be, and to **FIU-IND**.



- Pre-processing confirmation from the clients by way of oral confirmation or sign-in control for on line clients in place for transaction processing.
- Risk categorization of the clients is done based on their financial details and nature of business/ occupation. Review of such risk categorization is done periodically based on the change in client status, financial position, occupation etc. The parameters for categorizing the clients are also subject to review from time to time
- The transactions for which the alerts are generated are verified based on the knowledge about the clients' profile. For this purpose, fresh information sought from the clients regarding financial details/ net worth etc. periodically.

#### **(d) Policy for Acceptance of Clients**

The Company has developed customer acceptance policy and procedures which aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. Staff should adhere to following safeguards while accepting customers:

- No Trading account should be opened in a fictitious/benami name or on an anonymous basis, or in the name of a suspended/banned entity.
- No Trading account should be opened in the name of any person with criminal background.
- Members of the Company must not establish accounts or relationships involving unregulated money service businesses or unregulated businesses involved in gambling activities.
- No account should be opened if appropriate due diligence measures cannot be applied to a customer for want of verification of documents or on account of non-cooperation of the customer or due to non-reliability of the data/information furnished by the customer.
- In case an account is being opened & operated by an agent on behalf of Principal, it should be specified in what manner the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity/value and other appropriate details. Further the rights and responsibilities of both the persons (i.e. the agent-client registered with Company).

#### **Abans Initiative:**

Abans is strictly complying with all the KYC norms laid down by the regulators. As a risk management perspective, we developed a process of initial screening of all the new clients, on the basis of the details such as: Client type, residential status, nationality, and occupation and income details. The clients categorized with low risk profile, medium risk profile and High-risk profile. Categories of clients are reviewed periodically. The parameters for client profiling are not dynamic and subject to review from time to time.

Clients of Special Category are categorized as High-Risk Clients and their financial details and nature of business are updated on a periodical basis. Ongoing due diligence is carried out for the clients based on their risk profiling. **High Risk client's profile are reviewed every year. Medium Risk clients are reviewed once in 3 years and low risk clients are reviewed once in 5 years. Their risk category is revised based on such fresh details of the clients.**

**Abans may rely on 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 reliance shall be subject to the conditions specified under PMLA & SEBI circular/ guidelines.**

The guidelines relating to identification of Beneficial Ownership for clients other than individuals or trusts, for client which is a trust and for foreign investors with respect of controlling ownership interest and whether the person with controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the judicial person through other means are monitored regularly.

**5. Maintaining & Retaining Records (point No.6, & and 8 (Points 2.3, 2.4 & 2.5 of the Latest Circular))**

- (i) The Company shall maintain adequate records so as to enable it to demonstrate that appropriate initial and ongoing Customer Due Diligence procedures have been followed. To this end, Company shall maintain records of
- Client Identification Procedure
  - All documents collected at the time of client on-boarding
  - Customer Risk Profiling
  - Account Files
  - Business Correspondences
- (ii) Adequate records of all transactions should be maintained in order to permit reconstruction of transactions including the amounts, types of currency involved, the origin of funds received into customer's accounts and the beneficiaries of payments out of customer's accounts. To this end, the Company shall retain following information for the account of their customers in order to maintain a satisfactory audit trail:
- a. the beneficial owner of the account;
  - b. the volume of the funds flowing through the account; and
  - c. for selected transactions:
    - the origin of the funds;
    - the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
    - the identity of the person undertaking the transaction;
    - the destination of the funds;
    - the form of instruction and authority.
- (iii) The Company shall maintain record of following transactions as prescribed under Rule 3, notified under the PMLA:
- a. all cash transactions of the value of more than Rs.10 lakh or its equivalent in foreign currency;
  - b. all series of cash transactions integrally connected to each other which have been valued below Rs.10 lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rs.10 lakh;
  - c. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
  - d. all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.
- For the above transactions, Company shall also maintain following information:
- a. the nature of the transactions;
  - b. the amount of the transaction and the currency in which it is denominated;
  - c. the date on which the transaction was conducted; and
  - d. the parties to the transaction.
- (iv) The Company shall maintain records of all the reports made to the authorities and information provided to them;
- (v) The Company shall also maintain the results of any monitoring of transactions or account, which is

carried out.

- (vi) All records should be readily retrievable.
- (vii) The Company shall maintain all the above records for a period of 10 years (amended to 5 yrs. Vide SEBI Circular ***CIR/MIRSD/1/2014 dated March 12, 2014*** from the date of cessation of transactions between the Company and the client.
- (viii) In situations where the records relate to on-going investigations or transactions, which have been the subject of a suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

**Abans Initiative:**

Steps are taken to comply with the record preservation and maintenance requirements as per regulator guidelines. The following information as regards the accounts of the customers is retained in order to maintain satisfactory audit trail

- The beneficial owner account opening documents
- The identification documents of the clients with remarks of the verifying official
- The volume of the funds flowing through the account
- Communication with the clients regarding their transactions and identification
- Ledger details of the clients
- Instruction slip/ communication and other documents related to transactions.
- Any other documents /files as mandated by the regulators from time to time

The documents are maintained with renowned storage houses where retrieval of the same can be done quickly. The documents are maintained for a minimum period of 5 years as specified by SEBI. In the case of on-going investigation, the documents shall be maintained till it is confirmed that the case under investigation is closed. Proper back-up of the electronic data shall also be preserved.

In terms of the guidelines from SEBI (***Circular CIR/MIRSD/1/2014 dated March 12, 2014***), the records evidencing the identity of clients and beneficial owners including the related documents shall be maintained and preserved for a period of 5 years after the business relationship has ended or account closed. Likewise, the records and the related documents such as identity documents shall be maintained for a minimum period of 5 years from the date of closing of the account. The record of information related to transactions shall be preserved for a period of 5 years from the date of the transaction.

**6. Continuous Monitoring of Transactions & Identification of Suspicious Transactions/Activities (Point No.9 (Point 2.6 of the Latest Circular))**

- (i) The Company shall undertake appropriate scrutiny and monitoring of customers' account activity and transactions on an ongoing basis in order to identify any unusual and potentially suspicious activity. This is possible only when the Company's staff has an understanding of the normal activity of the client so that they can identify any deviant transactions/activities;

- (ii) Transactions and account activity involving customers categorized as high risk should be subject to enhanced monitoring.
- (iii) Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith –
- a) gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
  - b) appears to be made in circumstances of unusual or unjustified complexity; or
  - c) appears to have no economic rationale or bonafide purpose;
  - d) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

Some of the circumstances which may lead to suspicion and certain transactions which are deemed to be suspicious in nature are:

- False identification documents or identification documents which could not be verified within reasonable time;
- Non-face to face clients;
- Doubt over the real beneficiary of the account;
- Accounts opened with names very close to other established business entities;
- Suspicious background or links with known criminals;
- Large number of accounts having a common account holder, introducer or authorized signatory with no rationale;
- Unexplained transfers between multiple accounts with no rationale;
- Unusual activity compared to past transactions;
- Use of different accounts by client alternatively;
- Sudden activity in dormant accounts;
- Activity inconsistent with what would be expected from declared business;
- Account used for circular trading;
- Unusual or unjustified complexity in transactions;
- No economic rationale or bonafide purpose of transactions;
- Doubtful source of funds;
- Transfer of investment proceeds to a 3<sup>rd</sup> party;
- Transactions reflecting likely market manipulations;
- Suspicious off-market transactions;
- Transaction value just below threshold in an apparent attempt to avoid reporting;
- Large sums being transferred from overseas for making payments;
- Transactions inconsistent with the clients apparent financial standing;
- Inconsistency in the payment pattern by client;
- Block deal which is not at market price or prices appear to be artificially inflated/deflated;
- Cash transaction with customers;
- Unusual transactions by Clients of Special Category (CSC), businesses undertaken by offshore banks/financial services, businesses reported to be in the nature of export and import;
- Transactions in Commodities could be considered as suspicious if they are far away from the prevailing market price or theoretical market price and are accompanied with offsetting transactions without satisfactory explanations;
- Transactions of a client would be considered as suspicious if the client does not confirm the transactions, does not sign the ledger account confirmations, Commodities ledger confirmations or does not affect receipts or payments of moneys due for a considerably long period of time without satisfactory explanations;
- Customers with no discernible reason for using Company's services e.g. clients with distant addresses

who could find the same service nearer home or client's requirements not in the normal pattern of Company's business which could more easily be serviced locally;

- "Cold calls" by investors who are not known personally by the staff member or the market in general;
- Transactions not in keeping with the investor's normal activity, the financial markets in which the investor is active, or the investor's business;
- Buying and selling of Commodities with no discernible purpose or in unusual circumstances e.g. churning at the client's request;
- Large quantity or frequent buying & selling by clients in scrip categorized as "Trade for Trade" by Exchange;
- Large numbers of transactions of small amounts by the same client in the same security, first purchased and then sold, the proceeds being credited to an account different from the original account;
- Transactions not in keeping with normal practice in the market to which it relates, i.e. with reference to market size and frequency or at off-market prices;

(iv) The compliance department of the Company shall randomly examine a selection of transactions undertaken by clients to examine and comment on whether or not they are in the nature of suspicious transactions.

**(v) Source of Alert:**

- a) **System Dependent:** A broker must have system in place to generate alerts based on certain thresholds on the transactions of the client to identify suspicious transactions.
- b) **System Independent:** All Stock Brokers need to have a mechanism of raising alerts/triggers from employees, media reports, law enforcement agency queries etc. Efforts should be made to create awareness on reporting of unusual transactions

**(vi) Review and Management of Alerts**

- a) An element of subjectivity and application of mind of the Principal Officer (PO) is involved in the decision making process for reporting suspicious transactions.
- b) At the time of reviewing the alerts, the following aspects should also be considered:
  - Updated financial information of client details before filing an STR
  - Details of occupation of the client
  - Giving details of the scrip, price movement of the scrip, value of transaction, details of holding including duration and any corporate actions
  - Creating a Watch List of clients based on own experience, risk categorization, parties penalized by SEBI and related accounts

**(vii) Process for filing of STRs through FINnet**

- a) The PMLA and the PML Rules require every reporting entity (which includes stock brokers) to furnish prescribed reports, including suspicious transaction report (STR) to FIU-IND. The reports are to be furnished through the FINnet gateway portal (FINgate), covering prescribed details

**(viii) Red Flag Indicators (RFIs)**

- a) FIU-IND has identified certain RFIs, to be implemented by the Reporting Entity (REs) concerned for generation of alerts and identification of suspicious transactions.
- b) RFIs are to be analysed, and if appear to be suspicious, to be reported to FIU-IND
- c) FIU-IND has issued guidelines on RFIs vide **F. No. 9-6/AG-II/2012/ FIU-IND dated March 11, 2016** and **F. No. 9-2/2021/Intermediaries/FIU-IND dated July 21, 2022**

**7. Reporting of Transactions including Suspicious Transactions (Point No.10 (Point 2.7 of the Latest Circular))**

- (i) All staff members shall ensure that any transaction and/or activity which is believed to be suspicious is

reported to the Principal Officer who shall validate whether the transaction/activity is of suspicious nature or not. However, it should be ensured that there is no discontinuity in dealing with the client until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended or other action taken. Such customer's accounts should be reviewed in conjunction with the Principal Officer and a decision should be made as to whether it should be closed.

- (ii) In some cases, customers may abandon transactions on being asked to give some additional details/documents/information. It is clarified that staff shall report all such attempted transactions in Suspicious Transactions Report, even if they are not executed by customers, irrespective of the amount of the transaction.

**Abans Initiative:**

Abans has designated the "Principal Officer" besides the Compliance Officer. The designated Principal Officer is the Chairman of the company. He has access to all the documents and top Management including Board of Directors.

The name of the Principal Officer has been intimated to the Director-FIU and other regulators such as BSE, NSE, SEBI, etc. as required under their guidelines. He would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in the identification and assessment of potentially suspicious transactions. There is process in place to intimate the change in Principal Officer immediately in case of any change.

**In addition to the existing requirement of designation of a Principal Officer, Abans has also designated a Designated Director. The same has been intimated to the Director-FIU.**

Abans has also registered itself with FIU-IND for the purpose of uploading suspicious transactions online and the registration number is allotted.

## **8. Action on Reported Suspicious Transactions & Cash Transactions**

- (i) All reported suspicious transactions of any customer(s) with suspicious identity should be reviewed by the Principal Officer thoroughly. After thorough verification & confirmation of transactions which are suspicious in nature, the same should be immediately (not later than 7 days) reported to FIU, Ministry of Finance, New Delhi in writing.
- (ii) Where the Company or an employee is put on notice that a particular customer or a particular type of transaction should be treated with caution, then it may be necessary to review the accounts or transactions in question, for example:
  - When a transaction for a customer is identified as being suspicious, other transactions for that customer should be reviewed;
  - When a customer's activities on one account have been identified as suspicious the customer's other related accounts should be examined.
- (iii) In cases where it appears, or it is strongly suspected, that an account is being used for criminal purposes, it should duly scrutinized and once confirmed, the Account should be closed, subject to any advice by the regulatory authorities.
- (iv) Where a customer is subjected to more than one validated suspicious transaction/activity/report, then

serious consideration should be given to closure of the relevant account(s) and any other connected accounts. This decision should be reached by senior line management, Compliance Officer and Principal Officer.

- (v) Reporting to Financial Intelligence Unit – India (FIU-IND):  
Principal Officer of the Company shall act as a central reference point in facilitating onward reporting of transactions to FIU-IND and for playing an active role in the identification and assessment of potentially suspicious transactions. Principal Officer of the Company shall submit Cash Transaction Reports (CTRs) and Suspicious Transaction Reports (STRs) as prescribed under Rule 3, notified under the PMLA to:

**Director, FIU-IND,  
Financial Intelligence Unit-India,  
6<sup>th</sup> Floor, Hotel Samrat,  
Chanakyapuri, New-Delhi – 110021  
<http://fiuindia.gov.in/>**

and shall adhere to the following instructions given in FMC Circular no. ISD/AML/CIR-1/2008 dated December 19, 2008.

#### **9. Co-operation with Authorities**

- (i) The Company and its staff shall cooperate with Anti Money Laundering authorities and shall comply with requirements for reporting any suspicious transactions/activity. However, due regard must be paid to the Company's policy of maintaining customer confidentiality. Confidential information about customers may, therefore, only be given to the authorities when there is a legal obligation to do so.
- (ii) The Company and its staff shall strictly ensure that there is no "tipping-off" to customers about suspicious transaction report being made about their transactions/activities or that the authorities are looking into their transactions/activities. If such information is passed to a customer, it may seriously hamper the enquiry/investigation of the authorities.
- (iii) There may be occasions when the authorities ask for a suspect account to be allowed to continue to operate while they progress with their enquiries. In such cases, the Company would cooperate with the authorities, as far as possible, within the bounds of commercial prudence and applicable laws. Senior line management and Principal/Compliance Officer must always be kept aware of such instances.

#### **10. Hiring of Employees**

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

#### **Abans Initiative:**

Abans has adequate screening procedures in place to ensure high standards when hiring employees. Screening of all the employees is carried out to ensure that their name/ Pan does not match with any barred , notified entity, having criminal records or barred by the regulators. It identifies the key positions within the organization s and ensures that the employees taking up such key positions are suitable and

competent to perform their duties. Further, no candidate is selected who has ever been convicted of offence under Money Laundering Act or any other civil or criminal Act.

## **11. Training**

- (i) All new staff, whether permanent, temporary or on contract, who may be involved in handling customers' on-boarding, execution of transactions must receive suitable induction training to ensure that they fully understand their responsibilities under the Company's AML Policy & Procedures. Such training shall inter-alia cover following topics:
  - What is money-laundering?
  - Company's requirements and obligations under the AML Policy & Procedures.
  - Company's legal or regulatory requirements and the risk of sanctions/penalties for staff as well as the Company.
  - Reporting requirements as prescribed by SEBI.
  - The role played by Company's Principal/Compliance Officer in money laundering deterrence.
  - The need to protect the Company's reputation.
- (ii) Staff in high-risk areas should receive appropriate training to enable them to understand the anti-money laundering techniques which are likely to be used in their area, and to remind them of their personal responsibilities under the Policy and local legal requirements.
- (iii) Annual refresher training courses should be conducted for staff in high-risk areas to remind them of their responsibilities and alert them to any amendments to the Company's AML Policy & Procedures or local legal and/or regulatory requirements, as well as any new anti-money laundering techniques being used.
- (iv) **Our clients are educated on the company's PMLA Policy and Procedures and are updated periodically on any new developments in this regard through investor awareness programs.**

### **Abans Initiative:**

All employees are given initial training on PMLA guidelines at the time of induction for new joiners.

Ongoing training of ML/ FT procedures given to frontline, back office, compliance, risk management and staff dealing with new clients.

## **12. Monitoring and Review of the Company's AML Policy & Procedures**

- (i) The Company shall undertake regular monitoring of its operations through line management and/or Compliance to check that all businesses are complying with the Company's AML Policy & Procedures as well as local legal and regulatory requirements as prescribed under the PMLA and by SEBI.
- (ii) Operational and functional review work shall be undertaken by Compliance and/or Audit functions, as appropriate. Compliance Officer shall liaise with their relevant Audit function counterpart to arrive at appropriate review programme and responsibility.
- (iii) The level and frequency of monitoring and review work shall be undertaken having regard to materiality and risk in relation to the business and customer base.

## **13. Further Information**



Any queries or doubts concerning Company AML Policy & Procedures or any local legislation or regulation or Circulars or Guidelines relating to Anti Money Laundering and/or Combating Financing of Terrorism shall be referred to the Principal Officer of the Company.

#### 14. **Recent Amendments**

##### (i) **Compliance Related to AADHAAR Update**

- On June 01, 2017 **Central Government** in Consultation with the **RBI** hereby makes the following further Amendment to the Prevention of Money Laundering (Maintenance of Records) Rules, 2005
- Accordingly, **SEBI** has instructed Stock Exchanges to advise their Stock brokers to take necessary steps for linking of Aadhaar numbers with their Broking Account
- Stock broker are required to collect the Aadhaar w.r.t client category as mentioned below:
  - ✓ **Individual** – Client himself
  - ✓ **Company** - Managers, Officers or Employees holding attorney to transact on company's behalf
  - ✓ **Partnership Firm** – Person holding attorney to transact on Firm's behalf
  - ✓ **Trust** – Person holding attorney to transact on Trust's behalf
  - ✓ **Unincorporated association or Body of Individuals** – Person holding attorney to transact on its behalf
- Where an Aadhaar number has not been assigned to a client, the client shall furnish proof of application of enrolment for Aadhaar. The client shall submit the same within a period of six months from the date of the commencement of the account-based relationship
- **Stock broker are required to update Aadhaar in UCC Portal**
- The clients, eligible to be enrolled for Aadhaar and already having an account-based relationship with reporting entities prior to date of this notification, the client shall submit the Aadhaar number by **31st December, 2017**

**Note: If the client fails to submit Aadhaar by December 31, 2017 the said account shall cease to be operational till the time the Aadhaar number is submitted by the client. However, this directive is currently obsolete.**

Further SEBI vide its circular no. SEBI/HO/MIRSD/DOP/CIR/P/2019/123 dated November 05, 2019, entities in the securities market, as may be notified by the Central Government, shall be allowed to undertake Aadhaar Authentication under section 11A of the PMLA. SEBI Registered intermediaries for reasons such as online on-boarding of clients, customer convenience, increased efficiency and reduced time for client on-boarding would prefer to use Aadhaar based e-KYC facility to complete the KYC of the client.

**The Ministry of Finance (Department of Revenue) has recognized several reporting entities to perform Aadhaar Authentication via the gazette notification no. CG-DL-E-22042020-219106 dated April 22, 2020.**

##### **Abans Initiative:**

**Abans strives hard to get the Aadhaar numbers updated pertaining to its existing clients, specially the**

“active” ones in the UCC database of ALL the Exchanges (NSE, BSE, MSEI, and MCX & NCDEX) and the Depository (CDSL). Further for the NEW clients Abans has mandated the submission of Aadhaar number at the time of account opening itself.

Further for online on-boarding of clients through the e-KYC authentication facility under section 11A of the Prevention of Money Laundering Act, 2002, Abans has initiated registration to act as a sub-KYC User Agency (sub-KUA), being a SEBI registered entity, under a UIDAI registered KYC User Agency (KUA)

#### (ii) Compliance Related to C-KYC

- **Government of India** has authorized the **Central Registry of Securitization and Asset Reconstruction and Security interest of India (CERSAI)**, to act as, and to perform the functions of, the Central KYC Records Registry under the PML Rules 2005, including receiving, storing, safeguarding and retrieving the KYC records in digital form of a “client”
- As per the 2015 amendment to PML (Maintenance of Records) Rules, 2005, every reporting entity shall capture the KYC information for sharing with the Central KYC Records Registry in the manner mentioned in the Rules, as per the KYC template for ‘individuals’ finalized by CERSAI
- **SEBI** has issued circular no. CIR/MIRSD/66/2016 dated July 21, 2016 on operationalization of Central KYC Records Registry (CKYCR) wherein the registered intermediaries were directed to upload the KYC data with CKYCR, in respect of all Individual accounts opened on or after August 01, 2016
- Further, **Government of India** vide its letter dated October 04, 2016 has directed as follows with regard to KYC of existing and new individual clients
  - Registered intermediaries have to update their IT system as well as register all **new accounts** of individual in accordance with the CKYCR template, mandatorily by **October 31, 2016**
  - Intermediaries other than mutual funds may ensure 50% completion of uploading of **existing KYC** data by **November 30, 2016** and the remaining 50% of KYC data by **December 31, 2016**
- As per Prevention of Money-laundering (Maintenance of Records) Amendment Rules, 2015, Rule 9 (I) (1A), every reporting entity shall within **three 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 Registry.

#### **Abans Initiative:**

Abans got its individual “active” clients’ CKYC done. Further repeated reminders are being sent to the existing individual “dormant” clients who have been inactive. Again, for all NEW individual clients, Abans ensures CKYC of the NEW clients to be submitted within the prescribed deadline.

#### (iii) Compliance Related to KYC process through use of Technology

- 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.
- In terms of PML Rule 9 (16), every SEBI registered intermediary 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).

- In terms of Rule 2 (d) of Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 (PML Rules) “Officially Valid Documents” means the following:
  - ✓ a. the passport,
  - ✓ b. the driving license,
  - ✓ c. proof of possession of Aadhaar number,
  - ✓ d. the Voter's Identity Card issued by Election Commission of India,
  - ✓ e. job card issued by NREGA duly signed by an officer of the State Government and
  - ✓ f. the letter issued by the National Population Register containing details of name, address, or any other document as notified by the Central Government in consultation with the Regulator
- Further, Rule 9(18) of PML Rules states that in case OVD furnished by the investor does not contain updated address, the document as prescribed therein in the above stated Rule shall be deemed to be the OVD for the limited purpose of proof of address.
- PML Rules allows an investor to submit other OVD instead of PAN, however, in terms of SEBI circular no. MRD/DoP/Cir- 05/2007 dated April 27, 2007 the requirement of mandatory submission of PAN by the investors for transaction in the securities market shall continue to apply

**Abans Initiative:**

Abans has decided to tap the constant technology evolution which has taken place in the market and has initiated to set-up an innovative platform allowing investors to complete KYC process online. Abans at all points of time will strive to adhere to the PMLA compliances which govern the online KYC process through the use of technology.

\*\*\*\*\*