Background:

- Pursuant to recommendations made by Financial Task Force on Anti Money Laundering standards, SEBI and FMC has advised its intermediaries to comply with the laws enacted by providing guidelines vide notifications. Also the intermediaries are asked to ensure that proper policies are framed.

Money Laundering:

- Money laundering involves disguising financial assets so that they can be used without detection of the illegal activity that produced them. Through money laundering, the launderer transforms the monetary proceeds derived from criminal activity into funds with an apparently legal source.

- As per Section 3 of the Prevention of Money Laundering Act, 2002 enacted in the January 2003 and came to force on 1st July, 2005 defines Money Laundering as under:

- Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offense of money laundering.

Overview of Financial Intelligence Unit:

- Financial Intelligence Unit – India (FIU-IND) was set by the Government of India vide O.M. dated 18th November 2004 as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIUIND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

Implementation of this policy

Mr. SARAVANAN THANGAVEL, The Principal Officer (FIU) is responsible for

- Compliance of the provisions of the PMLA & AML guidelines
- Act as central reference point and play an active role in identification & assessment of potentially suspicious transactions
- Ensure that Alice Blue discharges its legal obligation to report its suspicious transactions to the concerned authorities.
- The objective of KYC (Know Your Customer) and CDD (Customer Due Diligence) guidelines is to enable the managers to examine and assess their customer's financial dealings from anti-money laundering perspective.

The main aspect of Customer Due Diligence Process means:

- Obtaining sufficient information about to the client in order to identify who is the actual beneficial owner of the securities or on whose behalf transaction is conducted.
- Verify the customer's identity using reliable, independent source document, data or information.
- Conduct on-going due diligence and scrutiny of the account/client to ensure that the transaction conducted are consistent with the client's background/financial status, its activities and risk profile

The Customer Due Diligence Process includes four specific parameters:

- Policy for Acceptance of Clients
- Client Identification Procedure
- Monitoring of transactions
- Tracking and reporting Suspicious Transactions

Customer Acceptance Policy (CAP)

- No account shall be opened in anonymous or fictitious/benami name(s).
- Parameters of risk perception shall be clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc., to enable categorization of customers into low, medium and high risk called Level

I, Level II and Level III respectively; Customers requiring very high level of monitoring e.g., Politically Exposed Persons (PEPs) may be categorized as High.

- The Employee shall collect documents and other information from the customer depending on perceived risk and keeping in mind the requirements of AML Act, 2002 and guidelines issued by RBI from time to time.

- The Employee shall close an existing account or shall not open a new account where it is unable to apply appropriate customer due diligence measures i.e., branch is unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of data/information furnished to the branch. The Employee shall, however, ensure that these measures do not lead to the harassment of the customer. However, in case the account is required to be closed on this ground, the Employee shall do so only after permission of Senior Official of their concerned Offices is obtained. Further, the customer should be given a prior notice of at least 30 days wherein reasons for closure of his account should also be mentioned.

- The Employee shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations, etc. RBI has been circulating lists of terrorist entities notified by the Government of India so that brokers exercise caution against any transaction detected with such entities. The Employee shall invariably consult such lists to ensure that prospective person/s or organizations desirous to establish relationship with the broker are not in any way involved in any unlawful activity and that they do not appear in such lists.

b) The KYC Officer/Track wizz Screening System shall categorize the risk based on the profile for each new customer based on risk categorization. The broker has devised a revised Composite Account Opening Form for recording and maintaining the profile of each new customer. Revised form is separate for Individuals, Partnership Firms, Corporate and other legal entities, etc. The nature and extent of due diligence shall depend on the risk perceived by the Persons. The Employee should continue to follow strictly the instructions issued by the Company regarding secrecy of customer information. The Employees should bear in mind that the adoption of customer acceptance policy and its implementation does not become too restrictive and should not result in denial of brokering services to general public, especially to those, who are financially or socially disadvantaged.

c) The risk to the customer shall be assigned on the following basis:

- Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk.

Low-Risk (Level I)

1. Salaried Individuals.
2. House Wife
3. Corporate which are providing financial details of the last two years and identity of the beneficial owner is disclosed.
4. Government employees and government owned companies.
5. HNI's who have respectable social and financial payments.
6. Businessman whose identity and source of wealth is easily identified and who is complying with maximum KYC disclosures.
7. Clients who do not fall in the above-mentioned points and who provide maximum information as per KYC.
8. In addition to the above, clients who have been introduced by branches / authorized persons and having faith in their genuineness.

Medium Risk (Level II):

- Customers that are likely to pose a higher-than-average risk to the broker may be categorized as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile etc; such as:

1. Persons in business/industry or trading activity where the area of his residence or place of business has a scope or history of unlawful trading/business activity.
2. Where the client profile of the person/s opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious. Clients delegating authority of operation of their trading & beneficial accounts to any of their immediate family members.
3. Trading and demat accounts of School /College students, or any kind of person under student category.
4. Trading and demat accounts of house wives may be treated as medium risk subject to verification and scrutiny.
5. Clients who have not given a proper or justifiable proof towards their nature of business and or involved in lending / investment /small finance /credit /syndication activities.

High Risk (Client of Special Category) (Level III)

The Employees may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers and Special category clients, especially those for whom the sources of funds are not clear. The examples of customers requiring higher due diligence may include.

1. Entities into foreign exchange business and non- resident customers.
2. High Net worth individuals whose identity and source of income or wealth is not identifiable.
3. Trusts, charities, NGOs, organizations receiving donations etc.,
4. Company's having close family shareholding or beneficial ownership
5. Firms with sleeping /dormant partners.
6. Politically Exposed Persons (PEPs).
7. Those with dubious reputation as per public information available, etc.
8. Clients originated /resided in high-risk countries as announced by respective authority from time to time.
9. Corporates with reserves and surplus balance is less than legitimate.
10. Clients against whom any action has been taken by SEBI/Stock Exchange or any other regulatory authority.
11. Clients residing in highly sensitive areas. For example, Naxalite regions, areas where dealing in narcotic drugs, immoral traffic, corruption, etc is highly predominant. This includes persons residing in UAE, Kashmir (India), Leh-Ladakh, Pakistan, Kuwait, Iran & Iraq, Bangladesh, Afghanistan etc..(Countries list shall be updated by Ministry of Home affairs from time to time)

Customer Identification Procedure {CIP} (FOR NEW CLIENTS)

- The objective is to have a mechanism in place to establish identity of the client along with firm proof of address to prevent opening of any account which is fictitious / benami / anonymous in nature.

Documents which can be relied upon:

- **PAN Card:** PAN card is mandatory and is most reliable document as only one card is issued to an individual and we can independently check its genuineness through IT website.

- **IDENTITY Proof:** PAN Card itself can serve as proof of identity. However, in case PAN card carries an old photograph of the holder, which does not match current facial features of the client; we should take other identity proof in form of Voter's Identity card, Passport, Ration Card or any Government/PSU/Bank issued photo identity card.

- **ADDRESS Proof:** For valid address proof we can rely on Voter's Identity Card, Passport, Bank Statement, Aadhaar Letter, Ration card and latest Electricity/telephone bill in the name of the client.

Documents to be obtained as part of customer identification procedure for new clients:

A. In case of individuals, one copy of the following documents has to be obtained:

- As PAN is mandatory, verify its genuineness with IT website and cross verify the PAN card copy with the original. Please put "verified with original" stamp as proof of verification.

- Other proofs for identity are Voter's Identity card, Passport, Ration Card or any Government/PSU/Bank issued photo identity card or any other document prescribed by the regulatory authorities.

- Address proof in the form of Voter's Identity Card, Passport, Bank Statement, Ration card and latest Electricity/telephone bill in the name of the client or any other document prescribed by the regulatory authorities.

B. In case of corporate, one certified copy of the following documents must be obtained:

- Copy of the Copy of the Registration/Incorporation Certificate

- Copy of the Memorandum & Articles of the Association

- Copy of the PAN card and the Director Index No. (DIN)

- Copy of the latest audited Annual Statements of the corporate client

- Latest Net worth Certificate

- Latest Income Tax return filed.

- Board Resolution for appointment of the Authorized Person who will operate the account.

- Proof of address and identity of Authorized Person

C. In case of partnership firm one certified following must be obtained:

- Registration certificate
- Partnership Deed
- PAN card of partners
- Authorization letter for the person authorized to open and operate the account Proof of identity and address of the authorized person
- Annual statement/returns of the partnership firm

D. In case of a Trust, one certified copy of the following must be obtained:

- Registration certificate
- Trust Deed
- PAN card
- Authorization letter for the entity authorized to act on their behalf
- Officially valid documents like PAN card, voters ID, passport, etc of person(s) authorized to transact on behalf of the Trust.

E. In case of unincorporated association or a body of individuals, one certified copy of the following must be obtained:

- Resolution of the managing body of such association or body of individuals PoA in favor of person authorized to transact
- Officially valid documents like PAN card, voters ID, passport, etc of the person(s) authorized to transact
- Any document required by ABC to establish the legal existence of such an association or body of individuals.

F. In case of an NRI account – Repatriable/non-repatriable, the following documents are required:

- Copy of the PIS permission issued by the bank
- Copy of the passport
- Copy of PAN card
- Proof of overseas address and Indian address

- Copy of the bank statement
- Copy of the demat statement
- If the account is handled through a mandate holder, copy of the valid PoA/mandate

G. Ultimate Beneficiary ownership identification

Determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted.

Corporate:
The beneficial owner is the natural person(s), who, whether acting alone or together has a controlling ownership interest.

More than 10% of shares, capital, or profits of the company
Right to appoint majority of the directors

Partnership firm:
The ownership of/ entitlement to more than 10% of capital or profits of the partnership Firm
The right to control the management or policy decision;

Trust:
The beneficiaries with 10% per cent or more interest in the trust ,settlor.

Unincorporated association or body of individuals
Ownership of or entitlement to more than 15%. of the property or capital or profits of such association or body of individuals

List of Designated Individual / Entity

- We are checking SEBI Debarred list before opening the account also checking UNRC Resolution through http://www.un.org/sc/committees/1267/. If any client's name appearing in the above enclosed list then such account will not be opened with us.

Monitoring of Transactions

- Continuous monitoring is an essential ingredient of effective KYC procedures and the extent of monitoring should be according to the risk sensitivity of the account. Alice Blue shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Transactions that involve large amount of cash inconsistent with the size of the balance maintained may indicate that the funds are being 'washed' through the account. High risk accounts shall be subjected to intensive monitoring.

- The Compliance Department shall ensure adherence to the KYC policies and procedures. Concurrent/Internal Auditors shall specifically check and verify the application of KYC procedures and comment on the lapses if any observed in this regard. The compliance in this regard shall be put up before the Meeting of the Board on quarterly intervals. All staff members shall be provided training on Anti Money Laundering. The focus of training shall be different for frontline staff, compliance staff and staff dealing with new customers.

Tracking and reporting Suspicious Transactions All are requested to analyze and furnish details of suspicious transactions, whether or not made in cash. It should be ensured that there is no undue delay in analysis and arriving at a conclusion.

- What is a Suspicious Transaction: Suspicious transaction means 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; or

- Appears to be made in circumstance of unusual or unjustified complexity; or

  Appears to have no economic rationale or bona fide purpose

Reasons for Suspicious:

Identity of client

- False identification documents

- Identification documents which could not be verified within reasonable time

- Non-face to face client

- Clients in high-risk jurisdiction

- Doubt over the real beneficiary of the account
- Accounts opened with names very close to other established business entities
- Receipt back of well -come kit undelivered at the address given by the client

Suspicious Background

- Suspicious background or links with criminals

Multiple Accounts

- Large number of accounts having common parameters such as common partners / directors / promoters / address/ email addresses / telephone numbers introducer or authorized signatory Unexplained transfers between such multiple accounts.

Activity In Accounts

- 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

Nature Of Transactions

- Unusual or unjustified complexity
- No economic rationale or bonafied purpose Source of funds is doubtful
- Appears to be case of insider trading
- Purchases made on own account transferred to a third party through an off-market transactions through DP account

Transactions reflect likely market manipulations Suspicious off market transactions

Value Of Transactions

- Value just under the reporting threshold amount in an apparent attempt to avoid reporting large sums being transferred from overseas for making

payments 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

Record Keeping:

- For the purpose of the record keeping provision, we should ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PLM act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars. Records to be maintained should be sufficient to permit reconstruction of individual transactions (including the amounts and type of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behaviour. Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing financial profile of the suspect's account. To enable this reconstruction, Organization should retain the following information for the accounts 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.
D. The origin of the funds;
E. The form in which the funds were offered or withdrawn, e.g. cash, cheques, etc;
F. The identity of the person undertaking the transaction;
G. The destination of the funds;
H. The form of instruction and authority.

Organization should ensure that all client and transaction records and information are made available on a timely basis to the competent investigating authorities.

Maintenance / Retention of the Records:

- Following are the Document Retention Terms should be observed:

1. All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period of EIGHT YEARS (8) from the date of cessation of the transaction.
2. Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should also be kept for the EIGHT YEARS (8) from the date of cessation of the transaction
3. Records shall be maintained in hard and soft copies.
4. All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period of EIGHT YEARS (8) from the date of cessation of the transaction.
5. Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence should also be kept for the EIGHT YEARS (8) from the date of cessation of the transaction.
6. Records shall be maintained in hard and soft copies.
7. In situations where the records relate to on-going investigation 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.

Third Party Reliance

- We are not relaying on any third party for new client registration and all our clients are sourced and verification carried out by our own employees only.

- Tracking and reporting Suspicious Transactions

- All are requested to analyse and furnish details of suspicious transactions, whether or not made in cash. It should be ensured that there is no undue delay in analysis and arriving at a conclusion.

What is a Suspicious Transaction: Suspicious transaction means 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; or
- Appears to be made in circumstance of unusual or unjustified complexity; or
- Appears to have no economic rationale or bona fide purpose.

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

The Stock exchanges and the registered intermediaries shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, they do not have any accounts in the name of individuals/entities appearing in the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council (UNSC). 2 In order to ensure expeditious and effective implementation of the provisions of Section 51A of UAPA, Government of India has outlined a procedure through an order dated February 02, 2021 (Annexure 1) for strict compliance. These guidelines have been further amended vide a Gazette Notification dated June 08, 2021 (Annexure 2).

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'.

All departments in our organization 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

"Compliance with Section 12A of WMD Act – Freezing of Assets of Designated Individuals / Entities"

Further Alice Blue Financial Services Private Limited shall comply with the provisions of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 and the procedure prescribed by the Government of India. The Company shall maintain and screen the Designated List of individuals/entities issued by the Government or United Nations Security Council and ensure that no financial assets, securities or services are made available to such persons. In case of any match or suspicion, the Company shall immediately freeze the assets, halt transactions and report the matter to the Central Nodal Officer, FIU-IND and SEBI in accordance with the prescribed procedure.

Maintain the **Designated List issued by the Government of India / UN Security Council**

Update the list **immediately upon any notification**

Sources include:

Ministry of Finance notifications
FIU-IND
SEBI circulars

Screening of Clients

At account opening / onboarding
During periodic KYC review
On real-time transaction monitoring
Against updated Designated Lists

Action in Case of Name Match

Immediately stop the transaction
Freeze the account / assets provisionally
Do not allow withdrawal, transfer, or trading
Inform Central Nodal Officer (CNO) without delay Email: dir@fiuindia.gov.in

Reporting to SEBI

__ sebi_uapa@sebi.gov.in

Filing of Suspicious Transaction Report (STR)

File STR with FIU-IND

Employees Hiring, Employees Training and Investor Education:

- Hiring of Employees: We shall have adequate screening procedures in place to ensure high standards when hiring employees, having regard to

the risk of money laundering and terrorist financing and the size of the business, we ensure that all the employees taking up such key positions are suitable and competent to perform their duties. The Company HR is instructed to cross check all the references and should take adequate safeguards to establish the authenticity and genuineness of the persons before recruiting. The department should obtain the following documents:

A. Photographs

B. Proof of address

C. Identity proof

D. Proof of Educational Qualification

E. Previous Employment Details.

Employees' Training:

- We have an ongoing employee training program conducted by our Principal Officer and Senior Management, Participation of all the Key Employees in the Seminars conducted by various Regulatory bodies from time to time, so that the members of the staff are adequately trained in AML and CFT procedures.
- All the Circulars issued by various Regulatory bodies including that of PMLA, are circulated to all the staff Members and the same are also being discussed in length, in the Training Program". Training program shall have special emphasis on frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

- Our training will include, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees" duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the firm's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for noncompliance with the PMLA Act.

Monitoring Employee Conduct and Accounts:

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the Principal Officer. We will also review

the AML performance of supervisors as part of their annual performance review. The Principal Officer's accounts will be reviewed by the Board of Directors.

Investors Education:

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

Customer Education

Implementation of KYC procedures requires Employees to demand certain information from the customers that may be of personal in nature or which have hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Therefore, the front desk staff needs to handle such situations tactfully while dealing with customers and educate the customer of the objectives of the KYC program

Principal Officer

The Principal Officer shall maintain close liaison with enforcement agencies, brokers and any other institutions that are involved in the fight against money laundering and combating financing of terrorism.

Principle Officer :

Mr SARAVANAN THANGAVEL

Corporate Office: No. 153/2, 3rd Floor, M.R.B.Arcade, Bagalur Main Road, Dwaraka Nagar, Yelahanka, Bengaluru – 560 063, Karnataka.

Email: Grievances@aliceblueindia.com

Contact No.9739179955

Designated Director:

Mr SidhaVelayutham Mohanamoorthy.

Corporate Office: No. 153/2, 3rd Floor, M.R.B.Arcade, Bagalur Main Road,

Dwaraka Nagar, Yelahanka, Bengaluru – 560 063, Karnataka

Email: Grievances@aliceblueindia.com.

Contact No: 9840992691

This PMLA Policy is prepared by Compliance Officer

Reviewed by our Principal Officer and Designated Director

This Policy was placed before in the Board and was approved on 20-02-2026