ANTI MONEY LAUNDERING POLICY

Update: Varsha Vichare	Review: Mr. Bimal Choksi	Revision Ashvin C Choksi
	CEO	**Principal Officer**
	Board Meeting held – 25/07/2024	

Applicability:

- A C Choksi Share Brokers Private Limited (ACCSBPL), SEBI Registered Intermediary (INZ000198136) & Depository Participant of CDSL (IN-DP-104-2015)

Amended with respect to:

- The PMLA Act, 2002 as modified and circulars, rules & guidelines issued
- thereof. SEBI/ HO/ MIRSD/ DOP/ CIR/ P/ 2019/113 October 15, 2019

  SEBI Circular and Directives including SEBI Master Circulars ref.

  SEBI/HO/MIRSD/DOP/CIR/P/2020/73 dated 24th April 2020.

  SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated 06th June 2024

Introduction

Parliament of India enacted Prevention of money laundering Act, 2002 (PMLA) to prevent money– laundering and to provide for confiscation of property derived from, or involved in, money laundering and for matters connected therewith or incidental thereto. The provisions of PMLA came into force on 1st July 2005. 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

Section 12 of PMLA, inter-alia, requires all intermediaries associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992 to maintain a record of all the transactions, the nature and value of which has been prescribed under the rules notified under the PMLA. Pursuant to this, Securities and Exchange Board of India (SEBI) issued Guidelines on Anti Money laundering Standards and various circulars from time to time to implement the provisions PMLA in the securities market and to prevent and impede money- laundering and combat financing terrorism.

A C Choksi Share Brokers Private Limited (hereinafter referred to as 'ACCSBPL' or 'the Company'), has adopted this Anti Money Laundering policy in accordance with the provisions of the PMLA Act and the rules made there under, SEBI and Circulars issued from time to time on this subject. The policy applies not only to money laundering, but also to terror financing.

Policy

The company shall endeavor at all times to comply, in letter and spirit, with the provisions of all relevant laws, rules, regulations, guidelines and circulars issued by regulatory authorities in relation to the anti-money laundering and the company's policies & procedures. To ensure that ACCSBPL' properly discharges its legal obligations to report suspicious transactions to the authorities, the Principal Officer 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 and shall have access to and be able to report to senior management at the next reporting level or the Board of Directors.

- Mr. Ashvin C. Choksi, who is the whole-time Director of ACCSBPL, was appointed as Principal Officer and the same has been intimate to FIU -IND and updated on FINNET gateway.
- Names, designation and addresses (including email addresses) in case of change in Principal Officer' including any changes therein shall also be intimated to the Office of the Director - FIU. As a matter of principle, 'Principal Officer' of ACCSBPL will be of a sufficiently senior position and is able to discharge the functions with independence and authority.

** Appoint a Designated Director to review the implementation of compliance with PMLA Regulation
* * Establish appropriate 'Customer Due Diligence Process' for:
1. Identification of client (and actual beneficial owners) and verifications of their identity:
2. Obtaining additional 'know your client's information as appropriate and necessary:
3. Acceptance of clients:
4 Identification of suspicious transactions and reporting of the validated suspicions to the appropriate authorities as required:
** Maintain appropriate records of customer identification and trail transactions and co-operate with regulatory authorities to the extent required by the applicable laws and provide information as may be required. Without breaching the customer confidentiality agreement.

** Give appropriate training to the relevant staff for effective implementation of the AML policy & Procedures.
** The Company AML Policies & Procedures should be read in conjunction with the guidance set out in the organization.

Objective

The objectives of this policy are to:

1. **Prevent** an d detect the use of the C o m p a n y /company's services by money launderers or those involved in criminal activities including financing of terrorism and to protect the reputation of the company.

***** **Protect** the company and its employees a g a i n s t unfounded allegations of facilitating money launderingand terrorist financing; and

***** **Protect the** company and its employees against any criminal, civil and regulatory actions which might result from inadvertent involvement in money laundering and /or terrorist financing or from failure in operational controls.

Scope

The Policy sets minimum standards and applies to all staff and business activities of the Company.

Responsibility of Principal Officer & Line Management

The company shall appoint a Principal Officer, who shall be responsible for ensuring compliance with the provision of the PMLA and this AML Policy & Procedures. The company shall immediately intimate the name designation, address including email address of the Principal Officer to the Officer of the Director- FIU, 6th Floor, Hotel Samrat, Chanakya puri, N e w -Delhi -110021. Any change in the particulars of the Principal Officer shall also be immediately intimated to the Office of the Director-FIU.

From an operations standpoint, it is the responsibility of the Company's line management to ensure that their respective departments and staff are complying with the Company's AML policy & Procedures laid down, as well as local anti-money laundering legislation, standards and guidelines. The role of the Company's Principal Officer is to guide, advise and assist the line management in fulfilling their responsibilities in relation to anti-money laundering. Further, the Principal Officer shall be assisted by the Compliance Department in discharging these responsibilities towards ensuring compliance with the provisions of the PMLA and this policy. The Principal Officer shall have unrestricted access to the Company's Offices, IT Systems, and records in order to carry out his responsibilities.

Customer due Diligence Process

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

Procedure for Identification and Verification of customer:

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 shall be identified by the company using documents submitted along with KYC as per the regulatory guidelines and authentication will be done through in person verification by an employee/AP of ACCSBPL.
iv. The procedure to be followed for admitting a person as a client is as under:

***Client**/Client's Nominee/Company's Sales Executive should submit the account opening from/client registration duly filled–in and signed by the prospective client.

***The Member** - Client agreements should be executed together with the Risk Disclosure document **Client** should provide all the necessary information required along with the relevant documents.

The following documents should be collected from Non- Individual Clients:

1. Non-individual Client Registration Form.
2. Risk Disclosure Document.
3. All supporting documents for identity /address of the non-individual entity and the authorized signatory.
4. In the case of companies, a board resolution authorizing the directors/senior Employees /authorized signatory to operate on behalf of the company and to deal in the derivative market. In the case of other entities similar documents are required.
5. PAN Card copy of non-individual client and all the partner/directors in case client is a partnership firm or body corporate
6. Bank Account proof.

The following document are to be collected from **Individual:**

1. Individual Client Registration From.
2. Member & Client Agreement.
3. Risk Disclosure Document.
4. All other supporting documents for identity and residence of the individual.
5. PAN Card copy.
6. Bank account proof.
7. Aadhaar Card Copy

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

3. If all the documents and forms are in order, client should be allotted a Unique Client Code (UCC).

* Clients can start transacting only after they have been allotted UCC.

7. Submission of Aadhaar number

As per the SEBI new guidelines (Rules, 2005 has been amended as per the gazette notification dated June 1, 2017) for account opening of Individual /Non- Individual client where the client enters into an account-based relationship with Member. Further, it is provided that:

i. Where the client has not submitted Aadhaar number at the time of commencement of account-based relationship with the reporting entity, as per the PMLA requirement, then he/ it shall submit the same within 6 months of commencement of account-based relationship with the reporting entity.

ii. Similarly, where the client is already having an account-based relationship with reporting entities, prior to the date of notification, and has not submitted Aadhaar number as per

PMLA requirement to the reporting entity, then he/ it shall submit the same by December 31,2017. In case of failure submitting the documents within the aforesaid time limit, the account shall cease to be operational till the time Aadhaar.

Note: as per PML notification dated March 31, 2018 issued by Department of Revenue, Ministry of Finance pursuant to the interim order dated March 13, 2018 of Hon'ble Supreme Court, the Central Government has extended the date of submission of Aadhaar Number, and Permanent Account Number or Form 60 by the clients to the reporting entity till a date to be notified subsequent to pronouncement of final judgment in W.P. (C) 494/2012 etc.

As per new GR 2018, no Aaddhar copy is compulsory for account opening Trading and DP. As per Client wish he/ she can provide it for address proof.

iii. Prospective customers' identity should be verified using reliable, independent documentary and/or electronic source material. Where such evidence is not available the business should be declined.

iv. For information to be adequate to satisfy competent authorities in future that due diligence was observed by the Company of compliance with SEBI Guidelines, each original document should be seen prior to acceptance of a photocopy and all the documents should be self-certified by the customer.

Additionally, information that can be verified from the government websites like income tax etc. should be verified accordingly to establish the authenticity of the information given by the client. Where there are doubts about the quality or adequacy of previously obtained customer identification information for the existing customers then, based on materiality and risk category of each client, identification/verification should be carried out at appropriate time (i.e. Immediately - for high- risk customers, immediately - when a transaction of significance takes place, immediately - when there is a material change in the way in which the account is operated etc.)

vi. For non-individual customers e.g. companies (particularly private companies), trust, Partnerships, etc. measures should be undertaken to understand the ownership and control structure (including the person(s) who is/are able to exercise control over the funds) and appropriate identification and verification should be done.

Sr.	Client Category	Person
1	Individual	Client himself
2	Company	Manager, Officers or Employees holding. Attorneys to transact on company's Behalf.
3	Partnership Firm	Person holding Attorney to transact on firm's
4	Trust	Person holding Attorney to transact on Trust's
5	Unincorporated Association or body of	Person holding Attorney to transact on its Behalf.

vii As part of the due diligence measures sufficient information must be obtained in order to identify people who beneficially own or control securities accounts. Whenever it is apparent that the s e c u r i t i e s acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified and verified using client identification and verification procedures as early as possible. The beneficial owner is the natural person or person who ultimately owns, controls, or influences a client and / persons on whose behalf a transaction(s) is/are being conducted.

viii. It includes people who exercise ultimate effective control over a legal person or arrangement.

ix Before opening an account it must be ensured that the identity of the perspective client does not match with a person having known criminal background and that there are no prohibitory order sanctions against the prospective client by any enforcement/regulatory agency.

x. Before accepting any person as a client, it must be ensured that such not appear and does not linked in any way to the individuals and consolidate list of individuals and entities maintained by Security person's name does entities listed in the Council Committee established pursuant to United Nations Security Council Resolution 1267(1999).The consolidated list can be accessed from the UN website at http://www.un.org/sc/committees/1267/consolist.shtml.

All existing accounts should be scrutinized to ensure that no account is held by or linked to any of the individuals or entities included in the aforesaid consolidated list. The Company shall intimate full details of accounts bearing resemblance to any of the individuals/entities in the aforesaid consolidated list to SEBI and FIU-IND.

xi It must be ensured that no account, existing or new, bear any resemblance to designated individuals/entities mentioned in the schedule to the Government of India (Ministry of Home Affairs –Internal security-I Division) Order dated August 27, 2009 (as amended) under Unlawful activities (Prevention) Act, 1967.The updated list of such designated individual/entities would be communicated by SEBI from time to time.

In the event, particulars of any customer(s) match the particulars of designated individuals/entities listed in t h e said Scheduled, the Company shall, within 24 h o u r s , inform full particulars of the funds, financial assets or economic resources or relate services held in the form of securities, held by such customer in its books to the Joint Secretary (IS. I), Ministry of Home Affairs, at Fax No. 011-23092569 and also conveys over telephone on 011- 23092736. Such particulars apart from being sent by post shall be conveyed through email at jsis@nic.in. The company shall also send the particulars of the communication mentioned above through post/fax and through e-mail (sebi_uapa@sebi.gov.in)to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India, SEBI Bhavan Plot No.C4-A, "G" Block, Bandra Kurla Complex, Bandra (E), and 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.

In case the afore-mentioned details of any of the customers match the particulars of designated individuals/entities beyond doubt, the Company shall prevent designate people from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at

Fax No. 011-23092569 and also convey over telephone on 011-23092736.

The particulars apart from being sent by post shall be conveyed through e-mail at jsis@nic.in .

The Company shall also file the Suspicious Transactions Report (STR) with FIU-IND covering all transactions in such accounts, carried out or attempted, as per the prescribed format.

Company shall:

(i) Maintain the list of individuals/entities ("Designated List") and update it, without delay, in terms of paragraph 2.1 of the Order.

(ii) verify if the particulars of the entities/individual, party to the financial transactions, match with the particulars of the Designated List and in case of match, stock exchanges and registered intermediaries shall not carry out such transaction and shall immediately inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer ("CNO"), without delay.

The details of the CNO are as under:

The Director
FIU-INDIA
Tel.No.:011-23314458, 011-23314459 (FAX)
Email: dir@fiuindia.gov.in

xii. Non-Face-to-Face Customers: Company should apply Customer Due Diligence procedures ensuring that the process is equally effective for non-face-to- face customers & face-to-face customers. Financial services and products are frequently provided to face-to-face customers via telephone and electronic facilities, including the Internet. To mitigate the risks posed by such non-face-to-face business, customer due diligence, scrutiny of transactions and trading accounts should be conducted on an ongoing basis.

xiii. All material amendments or alterations to client information (e.g. financial information or standing instructions) should be affected only on receipt of written requests from the clients.

xiv. Company shall determine if the existing or potential client is a Politically Exposed person (PEP) by seeking additional information from clients, accessing publicly available information etc. If the existing/potential client is found to be PEP, approval should be obtained from the Whole-time Director of the Company to admit the PEP as client or to continue the existing business relationship. The Company shall also seek details of the source of funds of clients identified as PEP.

xv. A copy of client identification program should be forwarded to Director, FIU-IND, New- Delhi.

xvi 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, considering, where necessary, the client's source of funds; and

xvii. Clients are required to periodically update all documents, data, information or details of beneficial ownership submitted during the CDD process for updating their information.

xviii. Where the client has not submitted Aadhaar number at the time of commencement of account based relationship with the reporting entity, as per the PMLA requirement, then he/ it shall submit the same within 6 months of commencement of account based relationship with the reporting entity.

xix. Similarly, where the client is already having an account-based relationship with reporting entities, prior to the date of notification and have not submitted Aadhaar number, as per the PMLA requirement, to the reporting entity, then he/it shall submit the same by December 31, 2017

xx. In case of failure to submit the documents within the aforesaid time limit, the account shall cease to be operational till the time Aadhaar number is submitted by the client from 2018 Aaddhar no is not in compulsory documents. If the client wishes to provide it then only we accept it as Address proof

d) Be careful while accepting Clients of Special category:

We should be careful while accepting clients of special category like

a. Non-Resident clients
b. High net-worth clients, *
c. Trust, Charities, Non-Governmental Organization and organizations receiving donations.
d. Companies have close family shareholdings or beneficial ownership.
e. Politically Exposed Persons (PEP) Politically exposed people 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, government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. The additional norms applicable to PEP as contained in the subsequent parts of the circular shall also be applied to the accounts of the family members or close relatives of PEPs.
f. Companies offering foreign exchange offers.
g. Clients in high risk countries (like Libya, Pakistan and Afghanistan etc)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.
h. Non-face to face clients

I. Clients with dubious reputation as per public information available etc.
j. persons of foreign origin, companies having closed shareholding/ownership, companies dealing in foreign currency, shell companies, overseas entities, clients in high-risk countries, -
k. Current/Former Head of State, Current / Former senior high profile politician, - Or clients from high-risk countries
l. Clients belonging to countries where corruption/fraud level is high (like Nigeria, Burma, etc.)

Risk Profiling of Customer:

Risk profiling of all Customers shall 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

The categorization of the clients would be as under:

Risk Category	Type of account	Categorization based on Income	Status of
High	Non-Resident Accounts	Income more than Rs. 1 Crores p.a. or Net worth more than Rs. 50 crores.	Individual
High	1. Trusts 2. CIS 3. Partnership firms 4. Companies Where the shareholding structure is complex	Non-individuals whose income is more than Rs. 1 Crores p.a. or Net worth more than Rs. 100 crores.	on individual accounts
High / Medium	1. HUF 2. Companies other than above	**High:** Non-individuals whose income is more than Rs. 1 Crores p.a. or Net worth more than Rs. 100 crores. **Medium:** Non- individuals whose income is more than Rs. 50 Lakhs p.a. or Net worth more than Rs. 70 crores.	Non individual accounts
High / Medium	1. Housewives 2. Clients operating in F&O segment	**High:** HNI with income more than Rs. 1 Crores p.a. or Net worth more than Rs. 50 crores. **Medium:** Clients who have been found to be of some risk considering their trading background then may be classified as Medium. Additionally, HNI with income more than Rs. 50 Lakhs p.a. or Net worth more than Rs. 30 crores	Individual accounts

Medium / Low	Others	All Clients except for those covered above would be classified as low. Additionally, clients who are in above mentioned risk category but after a year of experience if found to be proper then they may be lowered to Low risk category as felt proper by the Principal officer in due discussion with the Designated director.	Individual / Non-Individual

i. In case of any account wherein alerts are observed on a regular basis, risk categorization would be increased based on the consensus of the Surveillance, Compliance Team and the compliance officer. Risk categorization can also be updated based on management view considering various risk parameters, in consultation with principal officer & compliance officer.

ii. The Company shall apply customer due diligence for clients on a risk sensitive basis i.e. Applicability of customer identification procedures, documentary requirements, ongoing account monitoring and 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.

Risk: Based Approach:

It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, the registered intermediaries shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that the registered intermediaries shall adopt an enhanced client due diligence process for higher risk categories of clients Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

Risk Assessment

The Company shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. registered intermediary shall identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and existing products. The Stock Exchanges and registered intermediaries shall ensure:

a. To undertake the ML/TF risk assessments prior to the launch or use of such products, practices, services, technologies; and

b. Adoption of a risk-based approach to manage and mitigate the risks.

Iii In certain limited circumstances, within the overall framework of the SEBI guidelines, the Company may apply reduced or simplified Customer Due Diligence measures for certain types of customer 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 cue program and to the Company's reputation, and who should and subject to enhanced Customer due diligence, include, but are not limited to the following:

1. 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

2 Private companies or public companies not subject to regulatory disclosure requirements and which are constituted in full or in part by bearer shares

3. Customers with complex account relationships e.g. multiple accounts in one
4. Non-Resident Clients
5. High Net-worth Clients
6. Trust, Charities, NGOs and organizations receiving donations
7. Companies having close family shareholdings or beneficial ownership
8. 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 Govt. senior politicians, senior Govt. /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
9. Companies offering foreign exchange offers
10 *Clients* in high-risk countries.

While dealing with clients from or situated in high-risk countries or geographic areas or when providing delivery of services to clients through high-risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspected, registered intermediaries apart from being guided by the FATF statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf_gafi.org from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude registered intermediaries from entering into legitimate transactions with clients from or situated in such high-risk countries and geographic areas or delivery of services through such high risk countries or geographic areas. The intermediary shall specifically apply EDD measures, proportionate to the risks, to business relationships and transactions with natural and legal persons (including financial institutions) from countries for which this is called for by the FATF.

11. Havens/sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent, Non face to face clients havens, count
12 Clients with dubious reputation as per public information available

(c) Policy for Acceptances 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 of terrorist financing Staff should adhere to the following safeguards while accepting customers:

4. 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.

5. No Trading account should be opened in the name of any person with criminal background and.

6. Members of the Company must not establish accounts or relationships involving unregulated service businesses or unregulated businesses involved in gambling activities.

7. No account should be opened if appropriate due diligence measures cannot be· applied to customer for without 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.

(d) Reliance on third party for carrying out Client Due Diligence (CDD)

i. Registered intermediaries may rely on a third party for the purpose of(a) identification and verification of the id entity of a client and(b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and

ii. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time. Further, it is clarified that the registered intermediary shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

(e)Continuous Monitoring of Transactions & Identification of suspicious Transactions/ Activities

i. The Company shall undertake appropriate scrutiny and monitoring of customers' accountancy 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 understands the nominal activity of the client so that they can identify any deviant transactions/activities.

ii. Transactions and accountancy activity involving customers categorized as high risk should be subject to enhanced monitoring.

iii. Suspicious transaction means ~ 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 complexity,

or

c. Appears to have no economic rationale or Bonafide purpose;

or

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 which could not be verified within a 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 opened with same account holders, same authorized signatories, same Introducers.
* 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 3rd 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 payments.
* Transaction inconsistent with the clients' apparent financial standing.
* Inconsistency in the payment pattern by client.
* Block deals which is not at market price or prices appear to be artificially inflated/deflated.
* Cash transactions 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 securities could be considered as suspicious if they are far away from the prevailing market price and are accompanied with offsetting transactions without satisfactory explanation.
* Transactions of a client would be considered suspicious if the client does not confirm the ransactions,does not sign the ledger account confirmations, securities ledger confirmations or does not affect receipts or payments of money 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.
* Transactions not in keeping with the "investor's normal activity, the financial markets in which the investor is active, or the investors. business; Buying and selling of securities 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 scripts categorized as 'Trade for Trade' by Exchange; Large numbers of transactions of small amount mounts 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 nor mal 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 examine the transactions undertaken by clients to examine and Comment on whether or not they are in the nature of suspicious transactions.

v. Any client found to be of suspicious of money laundering would be required to be additionally verified and additional due diligence will be carried out. All affiliates, associates, relatives for such client should also be reviewed so as to avoid risk of money laundering within the organization.

(f). Do not accept clients with identity matching persons known to have criminal background:

Check whether the client's identity matches 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 / regulatory agency worldwide.

KYC team shall check following sites before admitting any person as client:

- www.sebi.gov.in : for prosecution database and vanishing companies' database.
- www.fatf-gafi.org
- 1988-(Taliban) https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xsl t= htdoc s/resources/xsl/en/taliban.xsl
- 1267-(Al-qaida) https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt= htdoc s/resources/xsl/en/al-qaida.xsl
- 2140-(Yemen) https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt= htdoc s/resources/xsl/en/yemen.xsl
- 1718/2270- (North Korea) https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt= htdoc s/resources/xsl/en/dprk.xsl

7. Reporting of Transactions including Suspicious Transactions

i All staff members should 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 a 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 reports/suspicion. In exceptional circumstances, consent may not be given to continue operating the account, and transactions may be suspended or other action taken. Such customers' accounts should be reviewed i n conjunction n 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 should report all such attempted transactions in Suspicious Transactions Report, even if they are not executed by customers, irrespective of the amount of the transaction.

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. 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 transactions in question, for example:

* When a transaction for a customer is identified as being a customer, it should be reviewed.
* When a customer's activities on one account have been customers 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 /aactivity/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.

Designated/Principal Officer within the intermediary. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion. However, it shall be ensured that there is continuity in dealing with the client as normal until told otherwise and the client shall 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, in one or more jurisdictions concerned in the transaction, or other action taken. The Designated/ Principal Officer and

other appropriate compliance, risk management and related staff members shall have timely access to client identification data and CDD information, transaction records and other relevant information.

v. Reporting to Financial Intelligence Unit-India 73.In terms of the PML Rules, registered intermediaries are required to report information relating to cash and suspicious transactions to the Director,

Financial Intelligence Unit-India (FIU-IND) at the following address:

Director, FIU-IND,
Financial Intelligence Unit - India
6th Floor, Tower-2, Jeevan Bharati Building,
Connaught Place, New Delhi-110001, INDIA
Telephone : 91-11-23314429, 23314459
91-11-23319793(Helpdesk) Email: helpdesk@fiuindia.gov.in
(For FINnet and general queries)
ctrcell@fiuindia.gov.in
(For Reporting Entity / Principal Officer registration related queries)
complaints@fiuindia.gov.in
Website: http://fiuindia.gov.in

and shall adhere to the following instruction given in SEBI Circular no. ISD/AML/CIR-1/2008 dated December 19, 2008 while reporting; Cash Transaction. Reports (CTRs):

All cash transactions identified as per clause 7(iii) of this policy should be reported to the FIU- IND in

a) Cash Transaction Reports (CTRs):

- The CTRs (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month.
- The Company shall submit the CTRs in electronic format

- FIU-IND is in the process of developing technological infrastructure to enable submission of electronic return over a secure gateway.In the interim, the Company shall submit the CTRs in a virus-free CD.
- A label mentioning name of the Company(intermediary), SEBI Registration No., type of report (CTR), month and year of report should be affixed on the CD for the purpose of identification.
- CD should contain the following six data files:

1. CINCTL.txt (Control File)- Contains a summary of the data contained in the other 5 files.
2. CINBRC.txt (Branch Data File) - Contains details of the branches for which cash transactions are being reported.
3. CINACC.txt (Account Data File)– Contains details of accounts containing cash transactions.
4. CINTRN.txt (Transaction Data File)-Contains details of cash transactions
5. CININP.txt (Individual Data. File) - Contains details of individuals who are accountholders for whom cash transactions are being reported. Also details of Directors /Partners /Members etc. of legal persons/entities which are accountholders. Also contains the details of introducers. Authorized signatories and guarantors (if any) of the account.
6. CINLPE.txt (Legal Person/Entity Data File) - Contains details of legal persons/entities which are account holders for which cash transactions are being reported. Also contains the details of introducers, authorized signatories' guarantors (if any) of the account.

- The CD should be accompanied by Summary of Cash Transaction Report (format enclosed in Annexure 1 as provided by the regulator) in physical form duly signed by the Principal Officer. This summary should match the data in control File (CINCTL.txt).
- I n case the size of data files exceeds the capacity of one CD, the data files should be compressed by using WinZip 8.1 or Zip It Fast 3.0 (or higher version) compression utility. The detailed guidelines for preparation of data files, validation of data files and data structure of the six file formats mentioned above are given in Annexure 2 as provided by the regulator.

b)Suspicious Transaction Reports (STRs):

All suspicious transactions shall be reported by the Principal Officer to Director, FIU-IND within 7 working days of establishment of suspicion at the level of Principal Officer. The Principal Officer should record this reasons for treating any transaction by a series on transaction as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.

- The Principal Officer shall submit the STRs in electronic format.
- FIU-IND is in the process of developing teleological infrastructure to enable submission of electronic return over a secure gateway. In the interim, the Company shall submit the STRs in a virus-free CD;
- A label mentioning name of the Company (intermediary), SEBI Registration No., type of Report (STR), month and year of report should be affixed on the CD for the purpose of identification. The CD should contain the following six data files:

1. SINCTL.txt (Control File) - Contains a summary of the data contained in the other 5 files.
2. SINBRC.txt (Branch~ Data File) - Contains details of the branches for which suspicious transactions are being reported,
3. SINACC.txt (Account Data File)- Contains details of accounts containing suspicious transactions.
4. SINTRN.txt (Transaction Data file) Contains suspicious transactions' records.
5. SININP.txt (Individual Data File)–Contains details of individuals who are accountholders For whom suspicious transactions are being reported. Also contains details of Directors/Partners/Members etc. of legal people/entities which are accountholders. Also contains the details of introducers, authorized signatories and guarantors (if any) of the account.
6. SINLPE.txt (Legal Person/Entity Data File) – Contains details of legal persons/entities which are accountholder for which suspicious transaction are being reported. Also contains the details of introducer guarantors (if any) of the account.

* The CD should be accompanied by Summary of Suspicious (enclosed in Annexure 3 as provided by the regulator) in physical for duly signed by the Principal Officer. this summary should match with the data in Control file (SINCTL.txt).
* In case the size of data files exceeds the capacity of one CD, the date file should be compressed by using WinZip 8.1 or ZjpItFast 3.0 (or higher version) compression utility.
* The detailed guidelines for the preparation of the data files, validation of data files and data structure of the six file formats mentioned above are given in Annexure 4 as provided by the regulator.

7. a. **The Principal Officer** will be responsible for timely submission of CTRs and STRs FIU-IND:

   b. Utmost confidentiality should be maintained in filing of CTRs and STRs to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address

   c. No nil reporting needs to be made to FIU-IND in case there is no cash/suspicious transactions to be reported

8. **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 reports 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.

ii. 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 co-operate with the authorities, as far as possible within the group. ids of commercial prudence and applicable laws. Senior line management and Principal/Compliance Officer must always be kept aware of such instances.

9. Maintaining & Retaining Records

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., Company shall maintain records of

- * Client Identification procedure
- * All documents connected with the time of client on- boarding
- * Customer Risk Profiling
- * Account Files
- * Business Correspondences

ii. Adequate records of all transactions should be maintained to permit the 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 accounts of their customers in order to maintain a satisfactory audit trail:

1. The beneficial owner of the account.
2. The volume of the funds flowing 'through the account; and
3. 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 purpose of the funds.
   - * The form of instruction and authority.

iii. The Company shall maintain a record of the 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 value 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) suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as demat account, security account maintained by the registered intermediary.

d) 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;

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered.

For the above transactions, the Company shall also maintain the following

. i.the nature of the transactions.
ii. the amount of the transaction and the currency in which it is denominated.
iii. the date on which the transaction was conducted; and
iv. the parties to the transaction.
v. The Company shall maintain records of all the reports made to the authorities and information provided to them.
vi. The Company shall also maintain the results of any monitoring of transactions or account, which is carried out.
vii. All records should be readily retrievable.
viii. The Company shall maintain all the above records for a period of 10 years from the date of cessation of transactions between the Company and the client.
ix. In situations where the records relate to on-going investigations or transactions, which have been the subject of suspicious transaction reporting, they should be retained until it is confirmed that the case has been closed.

10. Record Keeping

1. Registered intermediaries shall ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PMLA as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.
2. Registered Intermediaries shall maintain such records as are sufficient to permit reconstruction of individual t transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.
3. Shall 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 a financial profile of the suspect account. To enable this reconstruction, registered intermediaries shall retain the following information for the accounts of their clients 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. cheques, demand drafts etc.
* the identity of the person undertaking the transaction;
* the destination of the funds;
* the form of instruction and authority.

4. Registered Intermediaries shall ensure that all client and transaction records and information are available on a timely basis to the competent investigating authorities. Where required by the investigating authority, they shall retain certain records, e.g. client identification, account files, and business correspondence, for periods which may exceed those required under the SEBI Act, Rules and Regulations framed there-under PMLA, other relevant legislation, Rules and Regulations or Exchange byelaws or circulars.

5. More specifically, all the intermediaries shall put in place a system of maintaining proper reord of transactions prescribed under Rule 3 of PML Rules as mentioned below:
   i. all cash transactions of the value of more than rupees ten Lakh or its equivalent in foreign currency.
   ii. all series of cash transactions integrally connected to each other which have been valued below rupees ten 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 rupees ten Lakh;
   iii. all cash transactions where forged or counterfeit currency notes or banknotes have been used as genuine and where any forgery of a valuable security has taken place.
   iv. all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

11. Information to be maintained

Intermediate firms are required to maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

I. the nature of the transactions.
II. the amount of the transaction and the currency in which it is denominated.
III. the date on which the transaction was conducted; and
IV. the parties to the transaction.

12. Retention of Records

Records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence shall be maintained and preserved for a period of Five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later."

"Registered intermediaries shall maintain and preserve the record of documents evidencing the identity of its clients and beneficial owners (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents) as well as account files and business correspondence for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later."

In situations where the records relate to on-going investigations or transactions which have been the subject of suspicious transaction reporting, they shall be retained until it's confirmed that the case has been closed.

Records of information reported to the Director, Financial Intelligence Unit - India (FIU- IND): Registered intermediaries shall maintain and preserve the record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of the PML Rules, for a period of eight t years from the date of the transaction between the client and the intermediary.

13. Employees' Training / Employees' Hiring :
Training of employee

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 the 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, and 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.

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.

14. Investors Education

Implementation of AML/CFT measures requires intermediaries to demand certain information from investors which may be of personal nature or has hitherto never been called for Such information can include documents evidencing sources of funds/income tax returns/bank records etc. This 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 intermediaries to sensitize their clients about these requirements as the ones emanating from AML and CFT framework. Intermediaries shall prepare specific literature/pamphlets etc. so as to educate the client of the objectives of the AML/CFT program.

15. 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 a1l business are complying with the Company's AML Policy requirements as prescribed under the PMLA and by SEBI.

ii. Operational and functional review work shall be undertaken by Compliance and/or Audit Function as appropriate. Compliance Officer shall liaise with their relevant Audit function counterpart to arrive at appropriate review program and responsibilities.

iii. Having regards to materiality and risk in relation to the business and customer base the policy shall be reviewed once annually. It shall however, be reviewed earlier, in case of need being aroused by virtue of a relevant circular issued by the regulators

16. Further Information

Any queries or doubts concerning Company AML Policy & Procedures or any local legislation 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.

17. List of Designated Individuals/Entities

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

.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:

i. 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

ii. 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

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

As per the Section 51A in The Unlawful Activities (Prevention) Act, 1967 and amendments thereto they do not have any accounts in the name of individual / entities appearing in the list of

individual and entities, suspected of having terrorist links which are approved by and periodically circulated by the UNSC.
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). Corrigendum dated March 15, 2023, and April 22, 2024, have also been issued in this regard (Annexure 3) and (Annexure 4). The list of Nodal Officers for UAPA is available on the website of MHA.

(a) 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.

(b) 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;

(c) prevent the entry into or the transit through India of individuals listed in the
Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

ACCSBPL will ensure the effective and expeditious implementation of said Order.

19. Appointment of Designated Director

Mrs. Dipika Ashvin Choksi has been appointed as “Designated Director” of the company and the same has been intimated to FIU-IND.

20. Implementation of Aadhaar (UIDAI)

In subsequent to the circular no 20170817-36 Dated August 17,2017 as per Prevention of Money Laundering (Maintenance of Records) Rules, 2005 has been amended as per the gazette notification dated June 1, 2017 (copy enclosed as Annexure 1) , inter alia, to provide for submission of Aadhaar number, where the client enters into an account based relationship with reporting entity.

The implementation of above said notification has been done and we have set/adopted necessary process to fulfill the requirements for Aadhaar (UIDAI) Updating Activity for all our Active Clients , as mentioned in point no 7 in this Policy.

21. Deregistering a client

ACCSBPL may de-register the client account based on action taken by SEBI/NSE/BSE or being part of list of debarred entities published by SEBI/ Exchanges/ Various broker forums.

ACCSBPL may also initiate action for deregistering a client on basis of information found in sites of CIBIL or legal matter or if it is reasonably found out that client is having suspicious back ground, link with suspicious organization, trading rational is not justifiable or any other reason/ instance as may deem fit to the management in consultation with Principal Officer.

ACCSBPL shall have right to close out the existing positions; sell the collateral to recover its dues, if any, before de-registering the client.

22. Inactive/ Dormant Client Account

Client accounts will be considered dormant if the client does not trade for the period of one year in any of the segment for which account was activated during initial KYC. However, in case the request for reactivation of the account is made by the client through email, SMS, or letter or if client confirms existing KYC details then account will be considered as active.

Annexure I

IDENTIFICATION OF BENEFICIAL OWNERSHIP

With reference to SEBI/HO/MIRSD/DOS3/CIR/P/2018/104 dated 04-July-2018 whereby they have mandated all registered intermediaries to obtain, as part of their Client Due Diligence policy, sufficient information from their clients in order to identify and verify the identity of persons who beneficially own or control the securities account. The beneficial owner has been defined in the circular as the natural person or persons who ultimately own, control or influence a client and/or person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a legal person or arrangement.

Further, the Prevention of Money Laundering Rules, 2005 also require that every banking company, financial institution and intermediary, as the case may be, shall identify the beneficial owner and take all reasonable steps to verify his identity. The Government of India in consultation with the regulators has now specified a uniform approach to be followed towards determination of beneficial ownership.

Accordingly, we at A. C. Choksi Share Brokers Private Limited will comply with the following guidelines as prescribed:

A. For clients other than individuals or trusts:

Where the client is a person other than an individual or trust, viz., company, partnership or unincorporated association/body of individuals, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such person, through the following information:

The identity of the natural person, who, whether acting alone or together or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership means ownership of/entitlement to:

- more than 10% of shares or capital or profits of the juridical person, where the juridical person is a company.
- more than 15% of the capital or profits of the juridical person, where the juridical person is a partnership; or
- more than 15% of the property or capital or profits of the juridical person, where the juridical person is an unincorporated association or body of individuals.

In cases where there exists doubt as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interest s, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements or in any other manner. Where no natural person is identified as mentioned above, the identity of the relevant natural person who holds the position of senior managing official.

B.Forclient which is a trust:

Where the client is a trust, the intermediary shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

C. Exemption in case of listed companies:

Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

D. Applicability for foreign investors:

Intermediaries dealing with foreign investors' viz., Foreign Institutional Investors, Sub Accounts and Qualified Foreign Investors, may be guided by the clarifications issued VIDE SEBI circular CIR /MIRS D/11/2012 dated September 5, 2012, for the purpose of identification of beneficial ownership of the client.

In case of mutual funds, compliance of this circular shall be monitored by the Boards of the Asset Management companies and the Trustees and in case of other inter mediaries, by their Board of Directors.

Date: 21-08-2024