



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

B D SHAH SECURITIES LIMITED

R-701, Rotunda, Apollo Street, Fort, Mumbai – 400057

POLICY ON ANTI MONEY LAUNDERING

This Policy on Anti Money Laundering is the Property of M/s B D SHAH SECURITIES LIMITED and is confidential, no part, contents should be copied with prior approval of the undersigned.

This manual is prepared as per Prevention of Money Laundering Act laid down by Financial Investigation Unit of The Ministry of Finance.

I hereby approve the Policy on Anti Money Laundering

For B D Shah Securities Limited

Mitesh Bipin Shah

Director


Date: 24-11-2023

Place: Mumbai

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 1 Internal Use

| | | | |
|---|--|----------|------------|
|  | <h1>Policy on Anti Money Laundering</h1> | Issue No | Issue Date |
| | | 1.9 | 24/11/23 |

| |
|---------------------------------------|
| 1. Contents, Distribution, Amendments |
|---------------------------------------|

Contents:

| Sr. No | Title | Page No |
|--------|---|---------|
| 1 | Cover Page, Approval | 1 |
| 2 | Contents, Distribution List, Amendments | 2 |
| 3 | Policy on Anti Money Laundering | 4 |


Distribution List

| Sr. No. | Copy Type | COPY HOLDER | Location |
|---------|---|------------------------|------------|
| | | Designation | |
| 1 | Master Copy (Original & hard copy) and original soft copy | Ashish Shah, Director | Vile Parle |
| 2 | Soft read only copy on shared folder | All internal employees | Vile Parle |

Amendments Made till 01 / 1 / 2009

| No. | Nature of Amendment | Reason for amendment | Date of Amendment |
|-----|--|--|-------------------|
| 1 | Induction of point D | SEBI Master Circular CIR/ISD/AML/3/2010 | 16-04-2014 |
| 2 | Insertion of sub-point 3 in point C | SEBI Circular CIR/MIRSD/1/2014 | 21-04-2015 |
| 3 | Insertion of point h in CDD | SEBI Circular CIR/MIRSD/1/2014 | 21-04-2015 |
| 4 | Insertion / amendment in sub point d of Policy for acceptance of client | SEBI Circular CIR/MIRSD/1/2014 | 21-04-2015 |
| 5 | Insertion of sub-point 6.5 in record keeping | SEBI Circular CIR/MIRSD/1/2014 | 21-04-2015 |
| 6 | Insertion of sub point 3 in Designation of an officer for reporting | SEBI Circular CIR/MIRSD/1/2014 | 21-04-2015 |
| 7 | Insertion of Point D Freezing of funds, financial assets or economic resources or related services | CDSL Comm 2236 SEBI Circular ISD/AML/Cir-2/2009 | 22-04-2016 |

| | | |
|-----------------------------|--|-----------------------------|
| Reviewed by Mr. Ashish Shah | | Approved by Mr. Mitesh Shah |
| | | Page 2 Internal Use |

| | | | |
|---|--|----------|------------|
|  | <h2>Policy on Anti Money Laundering</h2> | Issue No | Issue Date |
| | | 1.9 | 24/11/23 |

| | | | |
|-----|---|--|------------|
| 8. | Insertion of sub point 4 to point no. II Client Identification Procedure | PML Rules 2005 duly amended as per Gazette notification dt. 01-06-2017 | 22-12-2017 |
| 9. | Insertion of Explanation of Controlling Ownership Interest in point 3 sub point C | CDSL/OPS/DP/POLCY/ dt. 25-01-2013 SEBI Cir: CIR/MIRSD/2/2013 dt. 24-01-2013 | 26-04-2018 |
| 10. | Insertion of point no. 6 in Client identification procedure | SEBI Circular # SEBI/HO/MIRSD/DOP/CIR/P/2019/123 November 05, 2019 | 20-11-2019 |
| 11. | Insertion of Point 3 in III (B) Suspicious Transaction Monitoring & Reporting | FIU: F No. 9-2-2021/Intermediaries/FIU-IND – Supplemental Guidelines for detecting suspicious transactions under rule 7(3) of Prevention of Money Laundering (Maintenance of Records) Rules 2005 | 30-08-2022 |
| 12. | Insertion in points | SEBI/HO/MIRSD/SEC-FATF/P/CIR/2023/0170 dated 13-10-2023 | |

| | | |
|-----------------------------|--|-----------------------------|
| Reviewed by Mr. Ashish Shah | | Approved by Mr. Mitesh Shah |
| | | Page 3 Internal Use |



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

B.D.SHAH SECURITIES LIMITED

POLICY ON ANTI MONEY LAUNDERING

1. The Objective

- a. Money laundering has now become one of the major concerns of international financial community. Money Laundering is not just an attempt to disguise money derived from illegal activities. Rather, money laundering is involvement in any transaction or series of transactions that seek to conceal or disguise the nature or source of proceeds derived from illegal activities, including drug trafficking, terrorism, organized crime, fraud and many other crimes.
- b. "Know Your Customer" (KYC) is the guiding principle behind the Anti-Money Laundering (AML) measures. It incorporates the "Know Your Customer" Standards & "Anti Money Laundering" Measures, hereinafter to be referred as "KYC Standards" and "AML Measures". The objective of is to "have in place adequate policies, practices and procedures that promote high ethical and professional standards and prevent the Company from being used, intentionally or unintentionally, by criminal elements". KYC Standards and AML Measures would enable the Company to know/ understand its customers, the beneficial owners in case of non-individual entities, the principals behind customers who are acting as agents and their financial dealings better which in turn will help the Company to manage its risks prudently.

2. SEBI Mandate

SEBI has mandated that KYC policy should be designed to combat Money Laundering and should cover the following

- (a) Communication of group* policies relating to prevention of money laundering and terrorist financing to all management and relevant staff that handle account information, securities transactions, money and customer records etc. whether in branches, departments or subsidiaries;

* "group" shall have the same meaning assigned to it in clause (cba) of sub-rule (1) of rule 2 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 as amended from time to time."

- (b) Customer acceptance policy and customer due diligence measures, including requirements for proper identification;
- (c) Maintenance of records;
- (d) Compliance with relevant statutory and regulatory requirements;
- (e) Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 4 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

- (f) Role of internal audit or compliance function to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.
- (g) Regularly (annually) review the policies and procedures **on a group basis wherever applicable** on the prevention of ML and TF to ensure their effectiveness. Further, in order to ensure the effectiveness of policies and procedures, the person(s) / **group** doing such a review shall be different from the one who has framed such policies and procedures
- (h) **BDS SL 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. BDS SL 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**
 - c) **BDS SL shall leverage latest technological innovations and tools for effective implementation of name screening to meet the sanctions requirements**

3. Guidelines of this KYC Policy lies in the below mentioned Procedures which are related to the overall 'Client Due Diligence Process':

- I. Policy for acceptance of clients
- II. Procedure for identifying the clients
- III. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

Customer Due Diligence

The customer due diligence ("CDD"), measures comprise the following:

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

(b) Obtaining sufficient information in order to identify persons who beneficially own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 5 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

(c) Verify the customer's identity using reliable, independent source documents, data or information;

(d) Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted;

Explanation: Controlling Ownership interest means ownership of / entitlement to:

| Type of Customer | Persons to be considered Beneficial Owners (BOs) |
|--|--|
| Public / Private Limited Companies | The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means. For this purpose: 1. "Controlling ownership interest" means ownership of/entitlement to more than 10 per cent of the shares or capital or profits of the company. 2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements |
| Partnership Firm | the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 10 per cent of capital or profits of the partnership. |
| Unincorporated association of persons or body of individuals | the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals. The Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the |

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 6 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

| | |
|--------------------------------------|--|
| | beneficial owner is the relevant natural person who holds the position of senior managing official. Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official. |
| Trust/ Foundation | The identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with ten per cent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and; where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities. |
| .Applicability for foreign investors | Registered intermediaries dealing with foreign investors' may be guided by SEBI Master Circular SEBI/HO/AFD-2/CIR/P/2022/175 dated December 19,2022 and amendments thereto, if any, for the purpose of identification of beneficial ownership of the client; |
| | |

(d) Verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c);

(e) Understand the ownership and control structure of the customer;

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 7 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

(f) 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 customer, its business and risk profile, taking into account, where necessary, the customer's source of funds; and

(g) BDSSL shall periodically update all documents, data or information of all customers and beneficial owners collected under the CDD process.

(i) Reliance on third party for carrying out Client Due Diligence:

- I. BDSSL may rely on a third party for the purpose of (a) identification and verification of the identity of a client (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 record keeping requirements in line with the obligations under the PML Act.
- II. Such reliance shall be subject to the conditions that are specified in rule 9(2) of the PMLA Rules and shall be in accordance with the regulations and circulars / guidelines issued by SEBI from time to time.

(j) BDSSL shall register the details of a client, in case of client being a non-profit organisation, on the DARPAN Portal of NITI Aayog, if not already registered, and maintain such registration records for a period of five years after the business relationship between a client and the BDSSL has ended or the account has been closed, whichever is later. [Non-profit organization" means any entity or organisation, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 (21 of 1860) or any similar State legislation or a Company registered under the section 8 of the Companies Act, 2013 (18 of 2013)]

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

Confidentiality requirement does not inhibit information sharing among entities in the group.

I. Policy for acceptance of clients:

A) Features of Clients Acceptance Policy

To develop customer acceptance policies and procedures on a group basis where applicable, for dealing with ML and TF reflecting the current statutory and regulatory requirements that aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. The following safeguards are to be followed while accepting the clients:

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 8 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

- a) No account is opened in a fictitious / benami name or on an anonymous basis.
- b) Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken. The parameters should enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of KYC profile. Risk assessment shall also take in to account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as the updated list individuals and entities who are subjected to sanction measures as required under various UN Security Council Resolution (these can be accessed at http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and <http://www.un.org/sc/committees/1988/list.shtml>)
- c) Documentation requirement and other information to be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002 and **PML (Maintaining of records) Rule 2005 duly amended as per the gazette notification dated June 1, 2017**, guidelines issued by RBI and SEBI from time to time.
- d) Ensure that an account is not opened where it is unable to apply appropriate clients due diligence measures / KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client, information provided is suspected to be non genuine, perceived non cooperation of the client in providing full and complete information. Should not continue to do business with such a person and file a suspicious activity report. It should also evaluate whether there is suspicious trading in determining in whether to freeze or close the account. Should be cautious, to ensure that, it does not return securities of money that may be from suspicious trades. However, should consult the relevant authorities in determining what action it should take when it suspects suspicious trading.
- e) The circumstances under which the client is permitted to act on behalf of another person / entity should be clearly laid down. It should be specified in what manner the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity / value and other appropriate details. Further the rights and responsibilities of both the persons (i.e the agent- client registered with the intermediary, as well as the person on whose behalf the agent is acting should be clearly laid down). Adequate verification of a person's authority to act on behalf the customer should also be carried out.
- f) Necessary checks and balance to be put into place before opening an account so as to ensure that the identity of the client does not match with any person having known criminal background or is not banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide .
- g) The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 9 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

B) Risk-based Approach

It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. As such, apply each of the customer due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is to adopt an enhanced customer due diligence process for higher risk categories of customers. Conversely, a simplified customer due diligence process may be adopted for lower risk categories of customers. In line with the risk-based approach, the type and amount of identification information and documents that should be obtained necessarily depend on the risk category of a particular customer.

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.

C) Clients of special category (CSC):

Such clients include the following.

- i. Non resident clients
- ii. High net-worth clients,
- iii. Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations
- iv. Companies having close family shareholdings or beneficial ownership
- v. in the subsequent para 5.5 of this circular shall also be applied to the accounts of the family members or close relatives of PEPs.
- vi. Companies offering foreign exchange offerings
- vii. **Politically Exposed Persons" (PEPs). PEP shall have the same meaning as given in clause (db) of sub-rule (1) of rule 2 of the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005. The additional norms applicable to PEP as contained in the subsequent paragraph 14 of the master circular shall also be applied to the accounts of the family members or close relatives / associates of PEPs**
- viii. Clients in high risk countries where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following – Havens/ sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent. While dealing with clients in high risk countries where the existence/effectiveness of money laundering control is suspect, **and** if the host country intermediaries apart from being guided by the financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), shall also independently access and consider other publicly available information. **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. Further If the host country does not permit the proper implementation of AML/CFT measures consistent**

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 10 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

with the home country requirements, BDSSL shall be required to apply appropriate additional measures to manage the ML/TF risks, and inform SEBI.

ix. Non face to face clients

x. Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and the intermediary shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

II. Client identification procedure:

The 'Know your Client' (KYC) policy should clearly spell out the client identification procedure to be carried out at different stages i.e. while establishing the Broker – client relationship, while carrying out transactions for the client or when there arises doubts regarding the veracity or the adequacy of previously obtained client identification data.

- 1) The client should be identified by using **reliable independent sources including data, documents or information. Where the client purports to act on behalf of juridical person or individual or trust, the BDSSL shall verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.** Adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship should be obtained.
- 2) The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed in compliance with the Guidelines. Each original document should be seen prior to acceptance of a copy.
- 3) Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority.
- 4) As per PML Rules 2005 duly amended as per Gazette notification dated 01-06-2017, Submission and Linking of Client's account with Aadhaar Number where the clients have / shall enter in to a relationship based account with BDSSL. Further provided that:
 - a) Where the client has not submitted Aadhaar number at the time of commencement of account based relationship with BDSSL, as per PMLA Requirements, then he/ she shall submit the Aadhaar number within 6 months from the account opening date
 - b) The existing clients may link their Aadhaar numbers before 31st March 2017 or the date as extended / prescribed by the Authority
 - c) In case of failure to submit the Aadhaar number, the account shall be deactivated until the Aadhaar number (along with valid Aadhaar card copy) is submitted.
- 5) SEBI has prescribed the minimum requirements relating to KYC for certain class of BDSSL from time to time. Taking into account the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, to frame own internal guidelines based on experience in dealing with clients and legal requirements as per the established practices. Further, continuous familiarity and follow-up where inconsistencies are noticed in the information provided should be maintained. The underlying principle should be to follow the principles enshrined in the PML Act, 2002, as well as the SEBI Act, 1992 so that there is awareness of the clients on whose behalf it is dealing.
- 6) e-KYC Authentication facility under section 11A of the Prevention of Money Laundering Act, 2002 by Entities in the securities market for Resident Investors Circular # SEBI/HO/MIRSD/DOP/CIR/P/2019/123 November 05, 2019 Entities in the securities

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 11

Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

market, as may be notified by the Central Government, shall be allowed to undertake Aadhaar Authentication under section 11A of the PMLA. SEBI Registered intermediaries for reasons such as online on-boarding of clients, customer convenience, increased efficiency and reduced time for client on-boarding would prefer to use Aadhaar based e-KYC facility to complete the KYC of the client. These entities would be registered with UIDAI as KYC user agency (“KUA”) and shall allow all the SEBI registered intermediaries / mutual fund distributors to undertake Aadhaar Authentication of their clients for the purpose of KYC through them. For detailed procedure SEBI Circular # SEBI/HO/MIRSD/DOP/CIR/P/2019/123 November 05, 2019 , should be referred.

Record Keeping

To ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

6.2 To maintain such records as are sufficient to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.

6.3 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 a financial profile of the suspect account. To enable this reconstruction, 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:
 - the origin of the funds;
 - the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
 - the identity of the person undertaking the transaction;
 - the destination of the funds;
 - the form of instruction and authority.

6.4 To ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities. Where appropriate, they should consider retaining certain records, e.g. customer identification, account files, and business correspondence, for periods which may exceed that required under the SEBI Act, Rules and Regulations framed there-under PMLA 2002, other relevant legislations, Rules and Regulations or Exchange bye-laws or circulars.

6.5 More specifically, all BDSSL shall put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 12 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

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

ii. all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency;

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.

iii. all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine or where any forgery of a valuable security or a document has taken place facilitating the transactions;

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

Where BDSSL does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which BDSSL shall close the account of the clients after giving due notice to the client.

Explanation: For this purpose, the expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under rules 3 and 9 of the Prevention of Money-laundering (Maintenance of Records) Rules, 2005.

6.5 BDSSL 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 five years from the date of transaction.

Retention of Records

A) The following document retention terms should be observed:

(a) All necessary records on transactions, both domestic and international, should be maintained at least for the minimum period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye- laws or circulars.

(b) 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 same period.

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

III. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

A. Monitoring of transactions

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 13 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

1 Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money laundering procedures. This is possible only if the intermediary has an understanding of the normal activity of the client so that they can identify the deviant transactions / activities.

2. Intermediary should pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose. The intermediary may specify internal threshold limits for each class of client accounts and pay special attention to the transaction which exceeds these limits.

3 The intermediary should ensure a record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority. Suspicious transactions should also be regularly reported to the higher authorities / head of the department.

4 Further the compliance cell of the intermediary should randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions or not.

5 BDSSL will implement group wide programmes for dealing with ML/TF, which shall be applicable, and appropriate to, all branches and majority owned subsidiaries of the BDSSL as under:

- a. policies and procedures for sharing information required for the purposes of CDD and ML/TF risk management;
- b. the provision, at group level compliance, audit, and/or AML/CFT functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This shall include information and analysis of transactions or activities which appear unusual (if such analysis was done); similar provisions for receipt of such information by branches and subsidiaries from these group level functions when relevant and appropriate to risk management; and
- c. adequate safeguards on the confidentiality and use of information exchanged, including safeguards to prevent tipping-off

B. Suspicious Transaction Monitoring & Reporting

1. To ensure to take appropriate steps to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:
 - a) Clients whose identity verification seems difficult or clients appears not to cooperate
 - b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
 - c) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 14 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

- d) Substantial increases in business without apparent cause ;
 - e) Unusually large cash deposits made by an individual or business;
 - f) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
 - g) Transfer of investment proceeds to apparently unrelated third parties;
 - h) Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export- import of small items.
2. Any suspicion transaction should be immediately notified to the Money Laundering Control Officer or any other designated 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 should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of the report/suspicion. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.
3. In furtherance to above red flag indicators / circumstances following are the additional Red Flag Indicators which may be checked for the suspicious transactions as per FIU's supplemental guidelines for detecting suspicious transactions under rule 7(3) of Prevention of Money Laundering (Maintenance of Records) Rules 2005:
- a. Single or multiple transfer of funds of more than Rs. 1 crore in a calendar month from multiple sources / accounts which are not reported as clients. (TM11)
 - b. Sudden increase in the funding amount of Margin trading Facility (MTF) Exposure by 50 % of the previous month where the value of MTF is above Rs. 10 crores (TM12)
 - c. Off-market transfer of securities to unrelated accounts (Accounts with same PAN, mobile, email, bank details and same family flag are related accounts) in the form of Off-market sale, Gift and donation where the value of debit transaction shall be above Rs. 25 lakhs and the transaction value exceeds 5 times the income range (TM13)
 - d. Off market credit / dematerialization of 50000 or more shares worth Rs. 25 lakhs and above by single transaction or series of transactions in an ISIN where 80% or more shares are debited by way of off-market transfers to 3 or more than 3 unrelated accounts in a span of 30 days in listed Equity Shares (TM13A)
 - e. Off-market transfer of 500,000 or more unlisted Equity shares with reason code 'Off-Market Sale', 'Gift' or 'Donation' in a single transaction or series of transactions within a period of 1 month (transfer made through account transfer cum closure module with reason code "transfer to own accounts" be excluded)
 - f. Off-market transfers of listed Equity shares having value of 5 lakhs and above with reason code "Family Account Transfer", "Gift", "Donation" where the transaction value exceeds 5 times the income range or net worth on higher side as updated by the BO
 - g. Off-market transfer of listed Equity shares with transaction value of Rs. 25 lakhs and above with reason code "Off-Market Sale" where the consideration value mentioned by BO is +/- 50% of prevailing market value of Equity Shares
 - h. Off-Market single or series of transactions having value of Rs. 2 lakhs and above in suspicious scrips for which unsolicited SMSs were circulated. The list will be available from below URLs

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 15 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

BSE: https://www.bseindia.com/attention_investors.aspx

NSE: <https://www.nseindia.com/regulations/unsolicited-messages-report>

- i. Accounts closed within 30 days of opening and single or series of debit transactions (On-market, Off-market including IDT Transfer) with value of Rs. 10 lakhs and above excluding transfer made through account transfer cum closure module with reason code “transfer to own accounts” or securities received in source account through transmission.

C. Designation of an officer for reporting of suspicious transactions

1. To ensure that BDSSL properly discharge their 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. Names, designation and addresses (including email addresses) of ‘Principal Officer’ including any changes therein shall also be intimated to the Office of the Director-FIU-IND. In terms of Rule 2 (f) of the PML Rules, the definition of a Principal Officer reads as under:

Principal Officer means an officer designated by BDSSL; Provided that such officer shall be an officer at the management level

2. The Principle Officer will be responsible for awareness and update of the Prevention of Money Laundering Act laid down by Financial Investigation Unit of The Ministry of Finance to all management and relevant staff that handle account information, securities transactions, money and customer records etc. whether in branches, departments or subsidiaries and Clients, from time to time in the form of updates on the website, Regular training programs and / or emails.

3. As per SEBI Circular No. CIR/MIRSD/1/2014 dated 12-03-2014, Mr. Mitesh B. Shah Director of the Company is appointed as Designated Director and the same is communicated to FIU-IND.

D. Freezing of funds, financial assets or economic resources or related services

The Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism.

For accounts which are frozen on our own account or on receiving order from authorities all document should be preserved until final disposition of case to the satisfaction of authorities.

E. Employees’ Hiring/Employee’s Training/ Investor Education

1. Employees Hiring

- i. To put in place adequate screening procedures while hiring employees.
- ii. To identify the key positions within the organization structures having regard to the risk of money laundering and terrorist financing and
- iii. To identify the size of business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

2. Employees Training

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 16 Internal Use



Policy on Anti Money Laundering

| Issue No | Issue Date |
|----------|------------|
| 1.9 | 24/11/23 |

To conduct training sessions on AML and CFT procedures for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients with specific focus on the role of employment from time to time.

3. Investor Education

Proper write up should be prepared so as to educate the customers about the objectives of AML / CFT program.

==End of Document==

Reviewed by Mr. Ashish Shah

Approved by Mr. Mitesh Shah

Page 17 Internal Use