MONEDO FINANCIAL SERVICES PVT. LTD.

KYC AND AML POLICY

Contents

- Applicability to branches and subsidiaries outside India
- KYC Policy for existing customers

19. Appointment of Principal Officer
20. Maintenance and Preservation of record
21. Reporting to Financial Intelligence Unit – India
22. General

1. INTRODUCTION:

The Reserve Bank of India has issued comprehensive guidelines on Know Your Customer (KYC) norms and Anti-Money Laundering (AML) standards and has advised all NBFCs to ensure that a proper policy framework on KYC and AML measures be formulated and put in place with the approval of the Board.

The objective of RBI guidelines is to prevent NBFCs being used, intentionally or unintentionally by criminal elements for money laundering activities. The guidelines also mandate making reasonable efforts to determine the identity and beneficial ownership of accounts, source of funds, the nature of customer's business, reasonableness of operations in the account in relation to the customer's business, etc. which in turn helps the Company to manage its risks prudently. Accordingly, the main objective of this policy is to enable the Company to have positive identification of its customers.

Accordingly, in compliance with the guidelines issued by RBI from time to time, the following KYC & AML policy of the Company is approved by the Board of Directors of the Company.

This policy is applicable to all categories of products and services offered by the Company.

2. SCOPE AND APPLICATION OF THE POLICY

The scope of this policy is:

- To lay down explicit criteria for acceptance of customers.
- To establish procedures to identify of individuals/non-individuals for opening of account.
- To establish processes and procedures to monitor high value transactions and/or transactions of suspicious nature in accounts.
- To develop measures for conducting due diligence in respect of customers and reporting of such transactions.

To fulfil the scope, the following four key elements will be incorporated into our policy:

- Customer Acceptance Policy
- Customer Identification Procedures
- Monitoring of Transactions
- Risk Management

3. CUSTOMER ACCEPTANCE POLICY

Definition of a Customer

- A person or entity that maintains an account and/or has a business relationship with the Company
- One on whose behalf the account is maintained (i.e. the beneficial owner)
- Beneficiaries of transactions conducted by professional intermediaries such as Stock Brokers
- Chartered Accountants, Solicitors etc. as permitted under the law, and
- Any other person or entity connected with a financial transaction which can pose significant reputation or other risks to the Company, say a wire transfer or issue of high value demand draft as a single transaction.

A "Person" shall have the meaning as defined under KYC policy of RBI (and any amendment

from time to time by RBI) which at present is as follows:

'Person' shall include:

a. an Individual;
b. a Hindu Undivided Family;
c. a Company;
d. a Trust
e. a Firm;
f. an association of persons or a body of individuals, whether incorporated or not;
g. every artificial juridical person, not falling within any one of the above person (a to e);
h. any agency, office or branch owned or controlled by any one of the above persons (a to f)

4. GUIDELINES FOR ACCEPTING CUSTOMERS

Following norms and procedures will be followed by the Company in relation to its customers who approach the Company for availing financial facilities. While taking decision to grant any one or more facilities to customers as well as during the continuation of any loan account of the customer, the following norms will be adhered to by the Company:

i. No loan account will be opened, and / or money will be disbursed in a name which is anonymous or fictitious or appears to be a name borrowed only for opening the loan account i.e. Benami Account. The Company shall insist on sufficient proof about the identity of the customer to ensure his physical and legal existence at the time of accepting the application form from any customer.
ii. Circumstances, in which a customer is permitted to act on behalf of another person /entity, shall be clearly spelt out in conformity with the established law and practices, as there could be occasions when an account is operated by a mandate holder or where an account may be opened by intermediary in a fiduciary capacity.
iii. The Company shall not open any account or give / sanction any loan or close an existing account where the Company is unable to apply appropriate due diligence measures arising due to any of the following circumstances:
    - The Company is unable to verify the identity of the customer
    - The customer without any valid or convincing reasons refuses to provide documents to the Company which are needed to determine the risk level in relation to the customer loan applied for by the customer and his paying capacity
    - Information furnished by the customer does not originate from the reliable sources orappears to be doubtful due to lack of supporting evidence.
    - Identity of the customer directly or indirectly matches with any individual terrorist orprohibited / unlawful organizations, whether existing within the country or internationally, or if the customer or beneficiary is found, even remotely, to beassociated with or affiliated to any illegal, prohibited or unlawful or terrorist organization as notified from time to time either by Govt. of India, State Govt. or any other national or international body / organization.
iv. Subject to the above-mentioned norms and caution, at the same time all the employees of Company will also ensure that the above norms and safeguards do not result in any kind of harassment or inconvenience to bona fide and genuine customers who should not feel discouraged while dealing with the Company.

The Risk Team shall, at the time of approving a financial transaction/activity, or executing any transaction, verify the record of identity, signature proof and proof of current address or addresses including permanent address of the customer. For co-lending loans, this shall be verified by the NBFC partner. The Company shall however maintain a repository of KYC documents of borrowers under the co-lending programme as well.

5. RISK LEVEL CATEGORIZATION

i. **Type of low risk customers**- individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorized as low risk. Illustrative examples of low risk customers may include government departments and government owned companies, regulators and statutory bodies, etc.

In such cases, the policy requires only the basic requirements of verifying the identity an location of the customer.

ii. **Type of medium or high-risk customers** - Customers that are likely to pose a higher than average risk to DMI may be categorized as medium or high risk depending on the customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. DMI will apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially those for whom KYC and AML Policy 12 the sources of funds are not clear. Examples of customers requiring higher due diligence may include

- (i) Trusts, charities, NGOs and organizations receiving donations,
- (ii) Companies having close family shareholding or beneficial ownership,
- (iii)Firms with 'sleeping partners',
- (iv) Politically exposed persons (PEPs) of foreign origin,
- (v) Non-face to face customers, and
- (vi) Those with dubious reputation as per public information available, etc. DMI has formulated an indicative list of customers and their respective risk categories. Please find attached as Annexure-A.

iii.

6. DUE DILIGENCE OF BUSINESS PARTNERS

The following due diligence must also be performed on prospective Business Partners.

A) Verify Identity:

i. Obtain and file legible copies of corporate formation and registration documents or publiccompany prospectuses and government filings.
ii. PAN card of the Directors etc.
iii. Wherever possible (in the case of privately owned entities), arrange for recommendation from legal counsel to the company.
iv. Wherever possible (in the case of privately owned entities), obtain from appropriate government entity confirmation of due incorporation and existence of the corporation.

B) Verify Source of Income:

i. Research for the Company details in available news or business databases and obtain allcorporate earnings information available.

The Company shall maintain files on each Business Partner with copies of all data obtained and memorialize in writing all the verification efforts. These files may be maintained electronically and should be accessible quickly when needed.

7. DUE DILIGENCE ON EMPLOYEES

The Company shall perform the following Due Diligence on Prospective Employees prior to their date of joining

A) Verify Identity:

i. Obtain originals of and file legible copies of identification documents that contain photographs of theindividual. Acceptable examples include:

- Passports (obtain all nationalities an individual may have)
- PAN card
- Driver's license
- UID or Physical Aadhaar card/letter or e-Aadhaar letter

B) Verify Domicile of Residence:

i. Example: Obtain copies of utility bill receipts or other form of objective verification of Residence, UID or Physical Aadhaar card/letter or e-Aadhaar letter (if the address provided by the customer is the same on the document submitted for identity proof)

C) Verify the previous year's Employment Record:

i. Obtain and call the previous employer to check the credentials of the prospective employee

ii. Check and verify the address of employee

D) Check References:

i. Obtain 2 or more professional employment references from the prospective employee.

ii. The prospective manager of the employee, or, the Human Resources department, must personally converse with the prospect's references The Company shall maintain files for each employee hired together with copies of all data obtained. These files may be maintained in electronic or physical form and should be accessible quickly when needed.

Further these files will be classified as confidential data and details contained therein shall notbe divulged for cross selling or any other purpose.

8. PURPOSEFUL IMPLEMENTATION

The purpose of adopting the above measures and norms while taking decisions on the issue of customeracceptance is twofold. Firstly, the Company should not suffer financially at later stage due to lack of proper due diligence exercise and lack of information which is the exclusive possession of the customers.

Secondly, to curb and prevent any such practice by the customers which is aimed to achieve

unlawful objectives or any other practice by which the financial institutions can be used to perpetuate any criminal or unlawful activities. However, at the same time, this policy does not aim or intend to deny the benefit of financial services to those who genuinely need such services / facilities due to real lack of their own sufficient financial resources.

9. CUSTOMER IDENTIFICATION PROCEDURE (CIP)

Customer identification means identifying the customer and verifying his / her identity by using reliable,independent source documents, data or information. The Company needs to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional and the purpose of the intended nature of relationship. Being risk perception, thenature of information / documents required would also depend on the type of the customer (individual,corporate etc.)

10. NEED FOR PHOTOGRAPHS

- In case of change in the authorized signatories, photograph of the new signatory should be obtained duly countersigned by the competent authorities of the concerned institution / organization;
- Where the account is operated by the letters of Authority or Power of Attorney Holder, photograph of the authority holder should be obtained duly attested by the Borrower / Depositor.

11. PROOF OF CUSTOMERS' ADDRESS

A detailed list of the features to be verified and documents that may be obtained from the Customers are given in "Annexure-1" of this policy document. A Photostat copy of the proofs mentioned in "Annexure-1" should be filed along with the loan application. In case of need, the Company Manager can depute an official to visit the account holder / loan applicant at the given address to satisfy about the genuineness of the address.

12. PROVISIONS UNDER PMLA

As per the provisions of Rule 9 of the Prevention of Money Laundering (Maintenance of Records of theNature and Value of Transactions, The Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005 (hereinafter referred to as PML Rules), the Company shall:

- At the time of commencement of an account-based relationship, identify its clients, verify their identity and obtain information on the purpose and intended nature of the business relationship and
- In all other cases, verify identify while carrying out:

  - ✓ Transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected,
  - ✓ Any international money transfer operations.

In terms of proviso to rule 9 of the PML Rules, the relaxation, in verifying the identity of the client within a reasonable time after opening the account / execution of the transaction, stands withdrawn.

Abiding by the provisions of Rule 9, the Company shall identify the beneficial owner and take all reasonable steps to verify his identity. The said Rule also require that the Company should

exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions to ensure that they are consistent with their knowledge of the customer, his businessand risk profile.

Customer identification requirements keeping in view the provisions of the said rule are given in "Annexure-2" for guidance of the Company.

13. MONITORING OF TRANSACTIONS AND MAINTENANCE OF RECORDS OF TRANSACTIONS

It is equally essential for the Company to have a clear knowledge and understanding about the normal working pattern and activity of the customer so that the Company can identify all such unusual transactions which would fall outside the normal transactions of the customer.

To achieve this purpose, ongoing monitoring is necessary. The extent of such monitoring will depend upon the level of risk involved in a particular account. Any transaction or activity of the customer which gives rise to suspicion will be given special attention. Such monitoring is important to keep a check on any act or omission of the customer which may amount to money laundering or support any act relating to use of finance for criminal activities.

14. SUSPICIOUS TRANSACTION REPORT (STR)

A suspicious transaction is one for which there are reasonable grounds to suspect that the transactionis related to a money laundering offence or a terrorist activity financing offence. A suspicious transaction can include one that was attempted. Throughout this guideline, any mention of a "transaction" includes one that is either completed or attempted.

"Reasonable grounds to suspect" is determined by what is reasonable in the circumstances, including normal business practices and systems within the industry.

There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. The context in which the transaction occurs or isattempted is a significant factor in assessing suspicion.

An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour.

Responsibility:

The Compliance Team in co-ordination with the Chief Risk Officer should review the STR Reports and finalize the transactions to be reported as STR and shall submit a report to the Board of Directors of the Company which shall be quarterly reviewed. The Compliance Team is responsible for reporting the same to FIU-IND. The following activities will be undertaken in the process of reporting suspicious transactions:

- Monitoring of large value and exceptional transactions based on alerts defined
- Liaison with Institutional Business Teams for responses / clarifications on STR alerts
- Escalation of suspicious transactions to respective business heads / product heads
- Filing Cash Transaction Report (CTR) with the FIU by 15th of subsequent month
- Filing Suspicious Transaction Report (STR) with FIU by 15th of subsequent month from date ofestablishing of suspicious transaction as per the FIU format in both electronic and manual form

- Scrutinizing sample of customer data against UNSCR and other negative lists as issued by NHB/ other Regulatory / Statutory entities from time-to-time and escalating the same to BusinessHeads.

15. CASH TRANSACTION REPORTS (CTR)

All individual cash transactions in an account during a calendar month, where either debits or credit summation, computed separately, exceeding Rupees Ten Lakhs or its equivalent in foreign currency, during the month should be reported to FIU-IND. However, while filing CTR, details of individual cash transactions below Rupees Fifty Thousand may not be indicated.

The Principal Officer should ensure submission of CTR for every month to FIU-IND before 15th of the succeeding month. CTR should contain only the transactions carried out by the Company on behalf of their clients/customers excluding transactions between the internal accounts of the Company.

16. COUNTERFEIT CURRENCY REPORT (CCR)

A separate Counterfeit Currency Report should be filed for each incident of detection of Counterfeit Indian currency. If the detected counterfeit currency notes can be segregated on the basis of tenderingperson, a separate CCR should be filed for each such incident. These transactions should be reported to Director, Financial Intelligence Unit, India by not later than the 15th of the succeeding month from the date of occurrence of such transactions.

All branches of the Company have been provided with machines for detection of fake notes. In the event any fake or counterfeit note is detected by branch staff, despite taking all precautions; then it must be noted in a cash register separately. Reporting of the case with full details like name of customer, amount, denomination, date - must be reported by branch manager to Compliance Department at HO with copy to National Head- Branch Business and Zonal Head.

Compliance to collate all the data and report to NHB / RBI under PMLA, as mentioned above.

17. MONITORING & REPORTING OF TRANSACTIONS

The Company will keep a continuous vigil, if any of the following acts or events is noticed in relation tothe customer's approach or behaviour while dealing with the Company:

1. Reluctance of the customer to provide confirmation regarding his identity
2. Loan money is used for the purpose other than the one mentioned in the sanction letter form and the real purpose is not disclosed to the Company
3. Customer forecloses the loan prior to the stated maturity
4. Customer suddenly pays a substantial amount towards partial repayment of the loan
5. Customer defaults regularly and then pays substantial cash at periodical intervals i.e. once in sixmonths.

The Company shall pay special attention to all complex, high-risk, unusually large transactions and all unusual or suspicious patterns which have no apparent economic or visible lawful purpose.

The Company may prescribe threshold limits for a particular category of accounts and pay close attention to the transactions that exceed the prescribed threshold limits. Keeping this

in view, the Company shall pay particular attention to the cash transactions which exceed the limits of Rs. 10 lakhs,either per transaction or credit and debit summation in a single month. This would include transaction where the customer by way repayment of loan, whether in part or full, deposit Rs. 10 lakhs and abovein cash. Such transactions shall be reported to the Risk Department and the Principal Officer appointedas per this policy. In such cases, the Company shall keep a close and careful watch on the subsequent mode of payments adopted by such customer.

Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall attract special attention of the Company. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through that account. Company shall ensure that proper record of all transactions and cash transactions (deposits and withdrawals) of Rs.10 lakhs and above in the accounts is preserved and maintained as required under the PMLA.

The Company shall maintain proper record of the following transactions:

- All cash transactions of the value of more than rupees Ten lakhs to its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been valued belowrupees Ten lakhs 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 lakhs;
- All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency;
- All suspicious transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of valuable security or a document has taken place facilitating the transactions;
- All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

The Company shall ensure that it continues to maintain proper record of all cash transactions (depositsand withdrawals) of Rs. 10 lakhs and above. The internal monitoring system shall have an inbuilt procedure for reporting of such transactions and those of suspicious nature whether made in cash or otherwise, to controlling / head office on a fortnightly basis.

The records shall be preserved in the following manner:

i) The nature of transactions
ii) The amount of the transaction and the currency in which it was denominated
iii) The date on which the transaction was conducted
iv) The parties to the transaction

The information in respect of the transactions referred to in clauses I, II and III referred above will be submitted to the Director - FIU every month by the 15th day of the succeeding month.

The information in respect of the transactions referred to in clause IV referred above will be furnishedpromptly to the Director - FIU in writing, or by fax or by electronic mail not later than seven working days from the date of occurrence of such transaction.

The information in respect of the transactions referred to in clause V referred above will be furnished promptly by the Director - FIU in writing, or by fax or by electronic mail not later than seven working days on being satisfied that transaction is suspicious.

Strict confidentiality will be maintained by the Company and its employees of the fact of furnishing / reporting details of such suspicious transactions.

As advised by the FIU-IND, New Delhi; the Company will not be required to submit 'NIL' reports in casethere are no Cash / Suspicious Transactions, during a particular period.

The required information will be furnished by the Company directly to the FIU-IND, through the designated Principal Officer.

High risk accounts shall be subjected to intensified monitoring. The Company shall set key indicators for such high risk accounts, taking note of the background of the customer, which will include country of origin, source of funds, the type of transactions involved (like accounts having unusual transactions,inconsistent turnover, etc) and other risk factors. Additionally, the Company shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligencemeasures basis the revised risk categories.

In addition to the Ordinary Monitoring Standards, any high-risk accounts should also receive the following monitoring:

- Conduct periodic (at least quarterly) reviews of all medium to high-risk accounts
- Create additional reports designed to monitor all transactions in an account to detect patternsof potential illegal activities
- Follow up on any expectations detected from the monitoring reports by contacting the accountowner personally to inquire about the unusual activity detected and regularly report status of account inquiries to Compliance Officer.

18. RISK MANAGEMENT

I. For effective implementation of KYC policy there will be a proper co-ordination, communication and understanding amongst all the departments of the Company. The Board of Directors shall ensure that an effective KYC program is put in place by establishing proper procedures and ensuring their effectiveimplementation. Heads of all the Departments will ensure that the respective responsibilities in relationto KYC policy are properly understood, given proper attention and appreciated and discharged with utmost care and attention by all the employees of the Company.

II. The Risk department of the Company will carry out quarterly checks to find out as to whether all features of KYC policy are being followed and adhered to by all the Departments concerned. The Risk Department shall sign off on the KYC documents for corporate entities, before every disbursement.

III. The Company shall also mandatorily include KYC adherence in its internal audit scope every quarter. For co-lending partners, the Company shall carry out sample quarterly KYC sample audit by independent audit firms to assess adherence with the KYC norms.

IV. The Company will conduct at regular intervals training programmes to impart training to its staff members regarding KYC procedures to ensure consistent and highest degree of compliance level.

V. The inadequacy or absence of KYC standards can subject the Company to serious risks especially reputational, operational, legal and concentration risks.

a. Reputational risk is defined as the risk of loss of confidence in the integrity of the institution,that adverse publicity regarding the Company's business practices and associations, whether accurate or not causes.

b. Operational risk can be defined as the risk of direct and indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.

c. Legal risk is the possibility that law suits, adverse judgments or contracts that turn out to beunenforceable can disrupt or adversely affect the operations or condition of the Company.

d. Concentration risk although mostly applicable on the assets side of the balance sheet, may affect the liability as it is also closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequencesfor the liquidity of the Company.

All these risks are interrelated. Any one of them can result in significant financial cost to the Company and diverts considerable management time and energy to resolving problems that arise.

19. POLICY IMPLEMENTATION GUIDELINES

Customer education

For implementing KYC policy, the Company shall have to seek personal and financial information from the new and intended customers at the time they apply for availing the loan facilities. It is likely that any such information, if asked from the intended customer, may be objected to or questioned by the customers. To meet such situation, it is necessary that the customers are educated and appraised about the sanctity and objectives of KYC procedures so that the customers do not feel hesitant or have any reservation while passing on the information to the Company. For this purpose, all the staff members with whom the customers will have their first interaction / dealing will be provided special training to answer any query or questions of the customers and satisfy them while seeking certain information in furtherance of KYC Policy. To educate the customers and win their confidence in this regard, Companymay arrange printed materials containing all relevant information regarding KYC Policy and anti-money laundering measures. Such printed materials will be circulated amongst the customers and in case of any question from any customer, the Company staff will attend the same promptly and provide and explain reason for seeking any specific information and satisfy the customer in that regard.

Introduction of new technologies

As part of the KYC and AML Policy, special attention should be paid to any money laundering threats that may arise from new or developing technologies including on-line transactions that might favour anonymity and adequate measures, if needed, should be taken to prevent their use in money laundering schemes. The Principal Officer should ensure to submit CTR,if any for every month to FIU-IND within the prescribed time schedule.

Applicability to branches and subsidiaries outside India

The KYC and AML Policy will also apply to the branches and majority owned subsidiaries of the Companylocated abroad, if any. When local applicable laws and regulations prohibit implementation of these guidelines, the same will be brought into the notice of RBI.

KYC policy for existing customers

Although this KYC Policy will apply and govern all the new and prospective customers; some of the KYC procedures laid down in this policy particularly which deal with Customer Identification, Monitoring ofTransactions and Risk Management can be effectively applied to the existing customers and their loanaccounts. While applying such KYC procedures to the existing loan accounts if any unusual pattern is noticed, the same should be brought to the notice of the Department Heads concerned and the Principal Officer appointed by the Company as per RBI directives.

In case any existing customer does not co-operate in providing the information required as

per KYC policy or conducts himself in such manner which gives rise to suspicion about his identity or credentials,such matters will be brought to the notice of Principal Officer who in turn will make necessary inquiriesand if required shall forward the name of such customers to the authorities concerned for appropriateaction. Besides above, in such situation the

Company, for reasons to be recorded, may recall the loan granted to such customers and take recourse to legal remedy against the customers as well as security furnished by such customers.

20. APPOINTMENT OF PRINCIPAL OFFICER

To ensure effective implementation of this KYC Policy and a proper co-ordination and communication between the Company and RBI and other enforcement agencies, the Company shall designate a senior official Principal Officer who will operate from the corporate office of the Company. The job of the Principal Officer will be to maintain an effective communication and liaison with RBI and otherenforcement agencies which are involved in the fight against money laundering and combating financing of terrorism, and to take appropriate steps in all such matters which are brought to the noticeof the Principal Officer by any department of the Company regard to any suspicious acts or omissions or acts of noncompliance on the part of any customers.

The name of the Principal Officer so designated, his designation and address including changes from time to time, may please be advised to the Director, FUI-IND.

Principal Officer shall be located at the Head / Corporate office of the Company.

21. MAINTENANCE AND PRESERVATION OF RECORDS

As per the provisions of PMLA, the Company shall maintain records as under:

a) Records of all transactions referred to in clause (a) of Sub-section (1) of section 12 read with Rule 3 of the PML Rules [referred to in Para 5. Supra] are required to be maintained for a period of ten years from the date of transactions between the Clients and the Company.

b) Records of the identity of all clients of the Company are required to be maintained for a period of ten years from the date of cessation of transactions between the Clients and the Company.

The Company will ensure that the appropriate steps are taken to evolve a system for proper maintenance and preservation of information in a manner (in hard and soft copy) that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities.

22. REPORTING TO FINANCIAL INTELLIGENCE UNIT - INDIA

The Principal Officer will report information relating to cash and suspicious transactions if detected, tothe Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PMLA rules, in the prescribed formats as designed and circulated by RBI at the following address:

Director, FIU-IND,

Financial Intelligence Unit, India,6th Floor, Hotel Samrat, Chanakyapuri,

New Delhi - 110021

Where the Principal Officer has reason to believe that a single transaction or series of transactions integrally connected to each other have been valued below the prescribed value to so to defeat the provisions of PMLA rules, such officer shall furnish information in respect of such transactions to the Director, FIU-IND, within the prescribed time.

A copy of all information furnished shall be retained by the Principal Officer for the purposes of officialrecord.

23. GENERAL

The Company shall ensure that the provisions of PMLA and the Rules framed thereunder and the Foreign Contribution and Regulation Act, 1976, wherever applicable, are adhered to strictly.

Where the Company is unable to apply appropriate KYC measures due to non-furnishing of informationand /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

Annexure A

Indicative list for Risk Categorization

High Risk

- Individuals and entities in various United Nations' Security Council Resolutions (UNSCRs) such as UN 1267 etc.;
- Individuals or entities listed in the schedule to the order under section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities;
- Individuals and entities in watch lists issued by Interpol and other similar international organizations;
- Customers with dubious reputation as per public information available or commercially available watch lists;
- Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk;
- Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions, etc.;
- Politically exposed persons (PEPs), customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
- Non-face-to-face customers;
- High net worth individuals;
- Firms with 'sleeping partners';
- Companies having close family shareholding or beneficial ownership;
- Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale;
- Shell companies which have no physical presence in branch locations. The existence simply of a local agent or low-level staff does not constitute physical presence;
- Accounts for "gatekeepers" such as accountants, lawyers, or other professionals for their clients where the identity of the underlying client is not disclosed to the Company; - Client Accounts managed by professional service providers such as law firms, accountants, agents,
- brokers, fund managers, trustees, custodians etc.;
- Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations; - Gambling/gaming including “Junket Operators” arranging gambling tours;
- Jewelers and Bullion Dealers; - Dealers in high value or precious goods (e.g. gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers);

- Customers engaged in a business which is associated with higher levels of corruption (e.g., arms manufacturers, dealers and intermediaries;
- Customers engaged in industries that might relate to nuclear proliferation activities or explosives;
- Customers that may appear to be Multi-level marketing companies etc;
- Individual who is a prisoner in jail

Medium Risk Customers

- Stock brokerage;
- Import / Export
- Gas Station
- Car / Boat / Plane Dealership
- Electronics (wholesale)
- Travel agency
- Telemarketers
- Providers of telecommunications service, internet café, International direct dialing (IDD) call service

Low Risk Customers All other customers (other than High and Medium Risk category) whose identities and sources of wealth can be easily identified and by and large conform to the known customer profile, may be categorized as low risk. In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.