IDBI BANK LTD.

POLICY

on

KNOW YOUR CUSTOMER (KYC) NORMS

and

ANTI-MONEY LAUNDERING (AML) MEASURES

INDEX

Glossary

RBI	Reserve Bank of India
CAP	Customer Acceptance Policy
CIP	Customer Identification Procedures
PML Act	Prevention of Money Laundering Act
CDD	Customer Due Diligence
FATF	Financial Action Task Force
CFT	Combating Financing of Terrorism
NOC	No Objection Certificate
PEP	Politically Exposed Person
POA	Power of Attorney
KYC	Know Your Customer
AML	Anti-Money Laundering

1. INTRODUCTION

1.1 Bank has in place a policy on KNOW YOUR CUSTOMER (KYC) norms and ANTI MONEY LAUNDERING (AML) measures approved by the Board in January 2006. The policy was based on then guidelines issued by RBI.

1.2 The KYC guidelines have regularly been revisited by RBI in the context of the recommendations made by the Financial Action Task Force (FATF) on Anti Money Laundering (AML) standards and on Combating Financing of Terrorism (CFT) and has advised banks to follow certain customer identification procedure for opening of accounts and monitoring transactions of a suspicious nature for the purpose of reporting it to appropriate authority.

1.3 RBI has advised banks to put in place a policy on 'Know Your Customer' and Anti-Money Laundering measures including the above referred recommendations with the approval of the Board.

1.4 RBI has issued the guidelines under Section 35A of the Banking Regulation Act, 1949 and Rule 7 of Prevention of Money-Laundering (Maintenance of Records of the Nature 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 and any contravention thereof or non-compliance may attract penalties under Banking Regulation Act.

1.5 This policy has been compiled taking into account cognizance of the guidelines enumerated in the Master Circular dated July 1, 2011 issued by RBI on Know Your Customer (KYC) norms/Anti-Money Laundering (AML) standards/Combating of Financing of Terrorism (CFT)/Obligation of banks under Prevention of Money Laundering Act, (PMLA), 2002, existing policy of the Bank on KYC and AML and the business strategies of the Bank.

2. OBJECTIVES OF THE POLICY

2.1 To lay down policy framework for abiding by the Know Your Customer Norms and Anti Money Laundering Measure as set out by Reserve Bank of India, based on the recommendations of the Financial Action Task Force (FATF) and the paper issued on Customer Due Diligence (CDD) for banks issued by the Basel Committee on Banking Supervision.

2.2 To prevent the Bank from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.

2.3 To enable the Bank to know / understand its customers and their financial dealings better, which in turn would help it to manage its risks prudently.

2.4 To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws / laid down procedures and regulatory guidelines.

2.5 To take necessary steps to ensure that the relevant staff are adequately trained in KYC/AML procedures.

3. SCOPE OF THE POLICY

3.1 This policy is applicable across all branches / business segments of the Bank, and its banking / financial subsidiaries and is to be read in conjunction with related operational guidelines issued from time to time. However subsidiaries would be guided by the instructions and guidelines issued from time to time by the respective regulators.

3.2 The contents of the policy shall always be read in tandem/auto-corrected with the changes/modifications which may be advised by RBI and / or by any regulators and / or by Bank from time to time.

4. DEFINITIONS

4.1 DEFINITION OF CUSTOMER

For the purpose of KYC policy, a 'Customer' is defined as :

- A person or entity that maintains an account and/or has a business relationship with the bank;
- One on whose behalf the account is maintained (i.e. the beneficial owner). [Ref: Government of India Notification dated February 12, 2010 - Rule 9, sub-rule (1A) of PMLA Rules - ' Beneficial Owner' means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercise ultimate effective control over a juridical person]
- Beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and
- Any person or entity connected with a financial transaction which can pose significant reputation or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

4.2 Definition of Money Laundering:

Section 3 of the Prevention of Money Laundering (PML) Act 2002 has defined the "offence of money laundering" as under:

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

5. KYC Policy Guidelines

There are four key elements to the KYC guidelines as set out by RBI

1. Customer Acceptance Policy;
2. Customer Identification Procedures;
3. Monitoring of Transactions; and
4. Risk Management

5.1 Customer Acceptance Policy (CAP)

The guidelines for Customer Acceptance Policy (CAP) for the Bank are given below:

i) No account should be opened in anonymous or fictitious/benami name. [Ref: Government of India Notification dated June 16, 2010 Rule 9, sub-rule (1C) - Banks should not allow the opening of or keep any anonymous account or accounts in fictitious name or account on behalf of other persons whose identity has not been disclosed or cannot be verified].

ii) No account would be opened or existing account would be closed if Bank is unable to apply appropriate customer due diligence measures i.e. Bank is unable to verify the identity and / or obtain documents required as per the risk categorisation due to non cooperation of the customer or non reliability of the data / Information furnished to the Bank. While carrying out due diligence it would be ensured that there in no harassment to the customer. The decision to close an account would be taken by the Branch Head after giving due notice to the customer, explaining the reasons for such a decision.

iii) While carrying out due diligence, it shall be ensured that the procedure adopted shall not become too restrictive and must not result in denial of banking services to general public, specially to those, who are financially or socially disadvantage.

iv) Before opening a new account, necessary checks shall be conducted so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc. A list circulated by RBI of persons with known criminal background or banned entities as well as a list of persons involved in frauds and deliberate default as per information available with the Bank shall be used for this purpose.

v) For the purpose of risk categorisation of customer, the relevant information shall be obtained from the customer at the time of account opening. While doing so, it shall be ensured that information sought from the customer is relevant to the perceived risk and is not intrusive. Any other information from the customer shall be sought separately with his/her consent and after opening the account.

Risk perception of different types of customers taking into account the background of the customer, nature of business activity, location of customer / activity and profile of his / her clients, country of origin, sources of funds, mode of payments, volume of turnover, social and financial status etc. shall be decided based on the relevant information provided by the customer at the time of account opening. The intensive due diligence would be required for higher risk customers, especially those for whom the sources of funds are not clear. An indicative risk categorisation of customers based on customer types is provided in **Annexure I**, which would be

reviewed periodically by the Standing Committee on KYC and AML of the Bank.

vi) A profile for each new customer shall be prepared based on risk categorisation. The customer profile shall contain information relating to customer's identity, social/financial status, nature of business activity, information about his clients' business and their location etc. The nature and extent of due diligence shall depend on the risk categorization of the customer. While preparing customer profile care shall be taken to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

Indicative information to be obtained from the customer at the time of opening of account for the purpose of creating customer profile is given in **Annexure II**. The information to be sought from the customer would be reviewed by Standing Committee of KYC and AML from time to time based on the guidelines issued by RBI / Bank and also depending upon business requirement and composition of the customers.

vii) Customers shall be accepted after verifying their identity as laid down in customer identification procedures. Documentation requirements and other information shall be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by RBI / Bank from time to time.

Indicative documentation required to be submitted by the customer at the time of opening of account is given in **Annexure III**. The

documentation requirements to be obtained from the customers would be reviewed by Standing Committee of KYC and AML from time to time based on emerging business needs and guidelines issued by RBI / Bank.

viii) Circumstances, in which a customer shall be permitted to act on behalf of another person/entity, as there could be occasions when an account is to be operated by a mandate holder or where an account is to be opened by an intermediary in fiduciary capacity, has also been spelt out in **Annexure III**.

5.2 Customer Identification Procedure (CIP)

5.2.1 The Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Sufficient information needs to be obtained to the satisfaction, which is necessary to establish, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Satisfaction means to be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

i) Customer Identification Procedure to be carried out at different stages

- while establishing a banking relationship (or)
- carrying out a financial transaction (or)
- when there is a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.

ii) Identity to be verified for:

- The named account holder
- Beneficiary account
- Signatories to an account
- Intermediate parties

iii) For customers that are natural persons, sufficient identification data shall be obtained to verify

- the identity of the customer,
- his / her address/location
- his / her recent photograph and
- document/s for verifying signature. In case no document is available for verification of the signature, Branch Head shall obtain the signature in his / her front. Alternately, identity documents can be substituted by satisfactory personal introduction except obtaining of photograph.

iv) For customers that are legal persons or entities -

- legal status of the legal person/entity through proper and relevant documents shall be verified;
- it shall be verified that any person purporting to act on behalf of the legal person / entity is so authorised and identify and verify the identity of that person;
- it shall be understood that the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

v) Whenever there shall be any suspicion of money laundering or terrorist financing or when other factors shall give rise to a belief that the customer does not, in fact, pose a low risk, full scale customer due diligence (CDD) shall be carried out before opening an account.

vi) When there shall be any suspicion of money laundering or financing of the activities relating to terrorism or where there shall be any doubt about the adequacy or veracity of previously obtained customer identification data, the due diligence measures shall be reviewed including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship.

vii) In case some close relatives, e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, as the case may be, want to open an account and utility bills, as required for address verification while opening the account, are not in their name, an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her can be obtained. Any supplementary evidence such as a letter received through post can be used for further verification of the address.

viii) Customer identification data (including photograph/s) shall be periodically updated after the account is opened. The periodicity of such updation shall not be less than once in five years in case of low risk category customers and not less than once in two years in case of high and medium risk categories.

ix) Permanent correct address, as referred to in **Annexure III**, means the address at which a person usually resides and can be taken as the address as mentioned in a utility bill or any other document acceptable for verification of the address of the customer.

5.2.2 Customer Identification – Guidelines in respect of few typical cases

i) Walk-in Customers

In case of transactions carried out by a non-account based customer, that is a walk-in customer, where the amount of transaction is equal to or exceeds rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. If there is a reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/-, identity and address of the customer shall be verified and filing a suspicious transaction report (STR) to FIU-IND may be considered.

[NOTE: In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 banks and financial institutions are required to verify the identity of the customers for all international money transfer operations]

ii) Trust/Nominee or Fiduciary Accounts

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. It shall be determined whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, receipt of satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting shall be insisted, as also shall obtain details of the nature of the trust or other arrangements in place. While opening an account for a trust, reasonable precautions shall be taken to verify the identity of the trustees and the settlors of trust (including any person settling assets into the trust), grantors, protectors, beneficiaries and signatories. Beneficiaries shall be identified when they are defined. In the case of a 'foundation', steps shall be taken to verify the founder managers/ directors and the beneficiaries, if defined.

iii) Accounts of companies and firms

Bank shall be vigilant against business entities being used by individuals as a 'front' for maintaining accounts. The control structure of the entity, determine the source of funds and identify the natural persons who have a controlling interest and who comprise the management shall be examined. These requirements may be moderated according to the risk perception e.g. in the case of a public company, Bank may not identify all the shareholders.

iv) Client accounts opened by professional intermediaries

a) If there is knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client would be identified. 'Pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds may be hold. 'Pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients may be managed. Where funds held by the intermediaries are not co-mingled and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners would be identified. Where such funds are co-mingled, the beneficial owners shall be looked through. Where the 'customer due diligence' (CDD) done by an intermediary is relied upon, Bank shall satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the KYC requirements. It may be noted that the ultimate responsibility for knowing the customer lies with the bank.

b) Under the extant AML/CFT framework, therefore, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits

disclosure of the client details, to hold an account on behalf of their clients. Bank shall not allow opening and/or holding of an account on behalf of a client/s by professional intermediaries, like Lawyers and Chartered Accountants, etc., who are unable to disclose true identity of the owner of the account/funds due to any professional obligation of customer confidentiality. Further, any professional intermediary who is under any obligation that inhibits Bank's ability to know and verify the true identity of the client on whose behalf the account is held or beneficial ownership of the account or understand true nature and purpose of transaction/s, should not be allowed to open an account on behalf of a client.

v) Accounts of Politically Exposed Persons (PEPs) resident outside India

a) Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Sufficient information on any person/customer of this category intending to establish a relationship shall be gathered and all the information available on the person in the public domain shall be checked. The identity of the person shall be verified and information about the sources of funds before accepting the PEP as a customer sould be sought. The decision to open an account for a PEP shall be taken by the concerned DGM or above / concerned Regional Head. Such accounts shall be subjected to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

b) In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, concerned DGM or above / concerned Regional Head shall approve to continue the business relationship and subject the account to the CDD measures

as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

c) Further, appropriate ongoing risk management procedures for identifying and applying enhanced CDD to PEPs, customers who are close relatives of PEPs, and accounts of which a PEP is the ultimate beneficial owner shall be applied.

vi) Accounts of non-face-to-face customers

With the introduction of telephone and electronic banking, increasingly accounts are being opened for customers without the need for the customer to visit the Bank Branch. In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, adequate procedures to mitigate the higher risk involved should be applied. Certification of all the documents presented should be insisted upon and, if necessary, additional documents may be called for. In such cases, first payment shall be effected through the customer's account with another Bank which, in turn, adheres to similar KYC standards. In the case of cross-border customers, there is the additional difficulty of matching the customer with the documentation and third party certification/introduction may have to be relied on. In such cases, it shall be ensured that the third party is a regulated and supervised entity and has adequate KYC systems in place.

vii) Accounts of proprietary concerns

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, the following documents shall be called for and verified before opening of accounts in the name of a proprietary concern:

a) Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc.

b) Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

c) These guidelines on proprietorship concerns apply to all new customers. In case of accounts of existing customers, the above formalities to be completed in a time bound manner.

VIII) Operation of bank accounts & money mules

a) "Money Mules" can be used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In some cases these third parties may be innocent while in others they may be having complicity with the criminals.

b) In a money mule transaction, an individual with an account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. When caught, these money

mules often have their accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a times the address and contact details of such mules are found to be fake or not up to date, making it difficult for enforcement agencies to locate the account holder.

c) Bank shall follow the guidelines on KYC / AML / CFT while opening of accounts and monitoring of transactions to minimize the operations of such mule accounts.

5.2.3 Alternatives / Approvals

No deviations or exemptions shall normally be permitted in the documents specified for account opening. For allowing the exceptions, suitable exceptions handling matrix may be prepared by concerned business group as per the requirement of the business in the overall ambit of RBI guidelines and should get it approved by the Standing Committee on KYC and AML. Once approved by the Standing Committee on KYC and AML, the authorities as per the matrix may allow the deviations and exceptions, if any.

All documents obtained for customer KYC shall be checked by the Branch official with the original documents and he / she shall give a confirmation to this effect in the copy of the documents. SOM / ASOM would scrutinize AOF & KYC documents for compliance of extant KYC norms of the Bank and sign the checklist accordingly. After satisfying himself / herself, the KYC shall be certified by Branch Head. Accounts would be opened by CPU / RPUs after the complete account opening form is received from the branches.

5.3 Monitoring of Transactions

a) Ongoing monitoring is an essential element of effective KYC procedures. Risk can be effectively controlled and reduced only if an understanding of the normal and reasonable activity of the customer is available to identify transactions that fall outside the regular pattern of activity. However, the extent of monitoring shall depend on the risk sensitivity of the account. Special attention shall be paid to all complex, unusually large transactions and all unusual patterns, which have no apparent economic or visible lawful purpose. The AML Cell shall generate the alerts for all such transactions for all high risk accounts as elaborated in **Annexure I**. As per the extant guidelines, branches also obtain details of the transactions, over and above specified limits, approved by the Board, from the customers in all the accounts for issuance of LCCs. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer shall attract special attention. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account. High-risk accounts shall be subjected to intensified monitoring. The AML cell shall generate the alerts for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. Bank shall put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers shall be carried out at a periodicity of **not less** than once in six months by the AML cell.

b) Ongoing due diligence with respect to the business relationship with every client shall be exercised and the transactions shall be examined closely in order to ensure that they are consistent with

their knowledge of the client, his business and risk profile and where necessary, the source of funds.

c) Any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above should be effected by debit to the customer's account or against cheques and not against cash payment. The provisions of Foreign Contribution (Regulation) Act, 1976 as amended from time to time, wherever applicable shall be strictly adhered to.

5.4 Risk Management

5.4.1 Banks is exposed to the following risks which arise out of Money Laundering activities and non-adherence of KYC standards.

- **Reputation Risk**

  Risk of loss due to severe impact in Bank's reputation. This may be of particular concern given the nature of the Bank's business, which requires the confidence of depositors, creditors and the general market place.

- **Compliance Risk**

  Risk of loss due to failure of compliance with key regulators governing the Bank's operations.

- **Operational Risk**

  Risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.

- **Legal Risk**

  Risk of loss due to any legal action the Bank or its staff may face due to failure to comply with the law.

5.4.2 For the purpose of effective implementation of KYC policy and AML Standards, Anti Money Laundering Cell headed by the Principal Officer shall monitor transactions in all customer accounts on concurrent basis with AML software and IT support to meet the requirements of KYC policy and AML standards. For instance, checking of negative list at the time of account opening, monitoring of transactions in customer accounts based on customer profile, customer type, nature of business / profession, number and value of transactions, different types of transactions, monthly turnover in the account, very large / suspicious transactions, transactions in new / dormant accounts etc. and draw various reports from historic data based on parameters defined etc.

5.4.3 All transactions of suspicious nature shall be reported to Principal Officer as an when the transactions are found to be suspicious by the branches. The Principal Officer of the Bank shall ensure that such reporting system is in place and shall monitor receipt of the reports.

5.4.4 The Standing Committee on KYC and AML shall review and set up various limits relevant for KYC and AML standards.

5.4.5 Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function would provide an independent evaluation of the Bank's own policies and procedures, including legal and regulatory requirements. Concurrent / Internal Auditors shall specifically check and verify the application of KYC procedures at the branches / CPU / RPU and comment on the lapses observed in this regard. The compliance in this

regard shall be put up before the Audit Committee of the Board on quarterly intervals.

5.5 The role and responsibilities for KYC verification

5.5.1 The basic check shall be done by the authorized branch officials at the branch level for all accounts. For High Risk customers, in addition to the authorized branch officials, the Branch Head shall verify the KYC. For all new Business Banking customers, Branch Head shall verify the KYC and ensure that accounts are monitored as per the guidelines of the Bank.

5.6 Accounts with Introduction

5.6.1 All the extant KYC Norms shall be applicable to the customers desiring to open Basic Banking "No Frills" accounts. In exceptional cases, where a person is not able to produce complete KYC documents, the Branch Head can exercise his discretion. The reasons for exercising the powers shall be clearly recorded by the Branch Head on the account opening form.

5.6.2 Although flexibility in the requirements of documents of identity and proof of address has been provided in the above mentioned KYC guidelines, a large number of persons, especially, those belonging to low income group both in urban and rural areas are not able to produce such documents to satisfy the bank about their identity and address. This leads to their inability to access the banking services and result in their financial exclusion. Accordingly, if a persons, who intend to keep balances not exceeding Rupees Fifty Thousand (Rs. 50,000/-) in all their accounts taken together and the total credit in all the accounts taken together is not expected to exceed Rupees One Lakh (Rs. 1,00,000/-) in a year and is not able to produce documents mentioned in **Annexure III**, may open an account, subject to:

Introduction from another account holder who has been subjected to full KYC procedure. The introducer's account with the Bank shall be at least six months old and should show satisfactory transactions. Photograph of the customer who proposes to open the account and also his address need to be certified by the introducer,

or

any other evidence as to the identity and address of the customer to the satisfaction of the bank.

5.6.3 While opening accounts as described above, the customer shall be made aware that if at any point of time, the balances in all his/her accounts with the bank (taken together) exceeds Rupees Fifty Thousand (Rs. 50,000/-) or total credit in the account exceeds Rupees One Lakh (Rs. 1,00,000/-) in a year, no further transactions will be permitted until the full KYC procedure is completed. In order not to inconvenience the customer, the customer would be notified when the balance reaches Rupees Forty Thousand (Rs. 40,000/-) or the total credit in a year reaches Rupees Eighty thousand (Rs. 80,000/-) that appropriate documents for conducting the KYC must be submitted otherwise operations in the account will be stopped.

5.7 Small Account

In terms of Government of India, Notification No. 14/2010/F.No.6/2/2007-E.S dated December 16, 2010, the Prevention of Money-laundering (Maintenance of Records of the Nature 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 has been amended.

A. Small Accounts

a) In terms of Rule 2 clause (fb) of the Notification, 'small account' means a savings account in a banking company where-

(i) the aggregate of all credits in a financial year does not exceed rupees one lakh;
(ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
(iii) the balance at any point of time does not exceed rupees fifty thousand .

b) an individual who desires to open a small account may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account.

Provided that –

(i) the Branch Head, while opening the small account, shall certify under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence;
(ii) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;
(iii) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk

scenarios, the identity of client shall be established through the production of officially valid documents; and

(iv) foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established through the production of officially valid documents,

B. Officially Valid Documents

a) The Notification has also expanded the definition of 'officially valid document' as contained in clause (d) of Rule 2(1) of the PML Rules to include job card issued by NREGA duly signed by an officer of the State Government or the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

b) Where the account has been opened relying **exclusively** on any of these two documents, viz. NREGA job card or Aadhaar letter, as complete KYC document for opening of an account, the account so opened shall also be subjected to all conditions and limitations prescribed above for small account.

5.8 Bank no longer knows the true identity

In the circumstances when it is believed that no longer Bank can be satisfied that it knows the true identity of the account holder, an STR with FIU-IND shall be filed.

5.9 Closure of accounts

Where Bank would be unable to apply appropriate KYC measures due to non-furnishing of information and / or non-cooperation by the customer, Bank shall consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decision would be taken by the Branch Head.

6 OBLIGATIONS UNDER PREVENTION OF MONEY LAUNDERING (PML) ACT 2002

Section 12 of PML Act 2002 issued by the Central Government, Ministry of Finance, Department of Revenue vide their notifications dated July 1, 2005 and subsequent notification, places certain obligations on every banking company, financial institution and intermediary, which include:

i) Maintenance of records of transactions
ii) Information to be preserved
iii) Maintenance and preservation of record
iv) Reporting to Financial Intelligence Unit – India

6.1 **Maintenance of records of transactions**: As per the PML Act, proper record of transactions prescribed under Rule 3 of PML Act has to be maintained properly. Details of transactions required to be kept as under PML Act are as under:

a) All cash transactions of the value of more than Rs. 10.00 lacs or its equivalent in foreign currency.
b) All series of cash transactions integrally connected to each other, which have been valued below Rs.10.00 lacs 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.10.00 lacs.
c) All transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency.
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 or documents has taken place facilitating the transactions.
e) All suspicious transactions whether or not made in cash and by way of cheques including third party cheques, pay orders, demand drafts,

cashier cheques, travelers cheques, account transfers, credits or debits into or from any non-monetary accounts (shares, demat accounts), money transfer or remittance, loans and advances, collection services etc.

6.2 **Information to be preserved** : As per the PML Act, all necessary information in respect of transactions referred to in Rule 3 of PML Act has to be maintained properly, to permit reconstruction of individual transaction, including the following information:

a) the nature of the transaction;
b) the amount of transaction and the currency in which it was denominated;
c) the date on which the transaction was conducted; and
d) the parties to the transaction

6.3 **Maintenance and Preservation of record** : Records containing information of all transactions including the records of transactions detailed in Rule 3 has to be maintained.

6.3.1 Data to be preserved in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Records to be maintained for at least ten years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

6.3.2 Records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) obtained while opening the account and during

the course of business relationship, are properly preserved for at least ten years after the business relationship is ended as required under Rule 10 of the Rules ibid. The identification records and transaction data should be made available to the competent authorities upon request.

6.3.3 Background including all documents/office records/memorandums pertaining to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level to be properly recorded. Such records and related documents to be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.

6.4 <u>Reporting to Financial Intelligence Unit – India</u> :

6.4.1 Information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to are required to be reported to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3.

6.4.2 The formats in which the transactions are to be reported are : i) Cash Transactions Report (CTR); ii) Summary of CTR iii) Electronic File Structure - CTR; iv) Suspicious Transactions Report (STR); v) Electronic File Structure - STR; vi) Counterfeit Currency Report (CCR); vii) Summary of CCR and viii) Electronic File Structure-CCR.

6.4.3 A profile for each customer based on the risk categorization shall be prepared. As a part of transaction monitoring mechanism, an appropriate

software application to put in place to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers.

6.5 Cash and Suspicious Transaction Reports

6.5.1 Cash Transaction Report (CTR)

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, the following instructions should be adhered to:

i) The Cash Transaction Report (CTR) for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis **(not on fortnightly basis)** and should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

ii) All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer to FIU-IND in the specified format not later than seven working days from the date of occurrence of such transactions (Counterfeit Currency Report – CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

iii) While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished.

iv) CTR should contain only the transactions carried out on behalf of clients/customers excluding transactions between the internal accounts of the bank.

v) A summary of cash transaction report for the Bank as a whole should be compiled by the Principal Officer every month in physical form as

per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

vi) Cash Transaction Reports (CTR) may be compiled centrally at one point for onward transmission to FIU-IND, provided:

a) The CTR is generated in the prescribed format;

b) A copy of the monthly CTR submitted on its behalf to FIU-India is available at the concerned branch for production to auditors/inspectors, when asked for; and

c) The instruction on 'Maintenance of records of transactions'; 'Information to be preserved' and 'Maintenance and Preservation of records' as mentioned above are scrupulously followed by the branch.

6.5.2 Suspicious Transaction Reports (STR)

i) While determining suspicious transactions, banks shall be guided by definition of suspicious transaction contained in PMLA Rules as amended from time to time.

ii) In some cases, transactions may be abandoned/aborted by customers on being asked to give some details or to provide documents. All such attempted transactions should be reported in STRs, even if not completed by customers, irrespective of the amount of the transaction.

iii) STRs shall be made if there are reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.

iv) The Suspicious Transaction Report (STR) shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his / her reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, Bank may consider the indicative list of suspicious activities contained in Annex-D of the 'IBA's Guidance Note for Banks, 2009'.

vi) No restrictions shall be put on operations in the accounts where an STR has been made. The fact of furnishing of STR shall be kept strictly confidential, as required under PML Rules. Customer shall not be tipped off at any level.

6.5.3 Non-Profit Organisation

The report of all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency shall be submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

7 Introduction of New Technologies – Credit cards/debit cards/ smart cards/gift cards

7.1 Appropriate KYC procedures shall be duly applied to customers using new technology driven products. Special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity shall be paid and if needed, necessary measures shall be taken to prevent their use in money laundering schemes.

7.2 Bank is engaged in the business of issuing a variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also shall be ensured.

7.3 Gift Cards shall be given to customers on submission of a respective Form duly filled and signed by the customer. KYC verification shall be done for Gift Cards on the basis of the form submitted by the customer as per the KYC & AML policy of the Bank.

7.4 Travel cards shall be given to the customers on submission of a concerned Form duly filled & signed by the customer supported by Passport and Visa which meets the KYC norms as per the KYC & AML Policy of the Bank.

8 Correspondent Banking

8.1 Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). These services include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing etc. These guidelines are not applicable to establishing Relationship Management Application (RMA) with correspondent banks. The establishment of RMA with correspondent banks shall be in terms of Bank's guidelines on exchange of RMA authorization.

8.2 Bank shall gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the services, and regulatory/supervisory framework in the respondent's country may be obtained. Similarly, Bank shall ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. Such relationships shall be established with the approval of ALCO and put up to the Board at its next meeting for post facto approval. The closing of such accounts shall be authorized by CGM-TBG and the same shall be reported to ALCO for information. The responsibilities of each bank with whom correspondent banking relationship is established shall be clearly documented. In the case of payable-through-accounts, the Bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The Bank shall also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request. A standard questionnaire, given in **Annexure IV**, has been prepared by the

Bank based on recommendations of Wolfsberg Group, which needs to be obtained before initiating the corresponding relationship. The following shall be ascertained while giving approval for opening of such accounts:

- Sufficient information to understand fully the nature of the business of the correspondent/respondent bank
- Information on the other bank's management,
- major business activities,
- level of AML/CFT compliance,
- purpose of opening the account,
- identity of any third party entities that will use the correspondent banking services,
- regulatory/supervisory framework in the correspondent's / respondent's country; and
- information from publicly available source whether that bank has been subject to any money laundering or terrorist financing investigation or regulatory action .

8.3 **Correspondent relationship with a "Shell Bank"**

A correspondent relationship with a **"**shell bank**"** (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group) shall not be entered. Shell banks are not permitted to operate in India. Bank shall not enter into relationship with shell banks and before establishing correspondent relationship with any foreign institution, shall take appropriate measures to satisfy that the foreign respondent institution does not permit its accounts to be used by shell banks. While continuing relationships with respondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing, extra caution shall be exercised. The respondent banks shall have anti money laundering policies and procedures in place and shal be applying enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

9 Wire Transfer

9.1 Bank is using wire transfers as an expeditious method for transferring funds between bank accounts. Wire transfers include transactions occurring within the national boundaries of a country or from one country to another. As wire transfers do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

9.2 The salient features of a wire transfer transaction are as under:

b) Wire transfer is a transaction carried out on behalf of an originator person (both natural and legal) through a bank by electronic means with a view to making an amount of money available to a beneficiary person at a bank. The originator and the beneficiary may be the same person.

c) Cross-border transfer means any wire transfer where the originator and the beneficiary bank or financial institutions are located in different countries. It may include any chain of wire transfers that has at least one cross-border element.

d) Domestic wire transfer means any wire transfer where the originator and receiver are located in the same country. It may also include a chain of wire transfers that takes place entirely within the borders of a single country even though the system used to effect the wire transfer may be located in another country.

e) The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the bank to perform the wire transfer.

9.3 Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can

be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, Bank shall ensure that all wire transfers are accompanied by the following information:

(A) Cross-border wire transfers

i) All cross-border wire transfers must be accompanied by accurate and meaningful originator information.

ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included.

iii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

(B) Domestic wire transfers

i) Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include

complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

ii) If bank has reason to believe that a customer is intentionally structuring wire transfer to below Rs. 50000/- (Rupees Fifty Thousand) to several beneficiaries in order to avoid reporting or monitoring, the bank must insist on complete customer identification before effecting the transfer. In case of non-cooperation from the customer, efforts would be made to establish his identity and Suspicious Transaction Report (STR) would be made to FIU-IND.

iii) When a credit or debit card is used to effect money transfer, necessary information as (i) above should be included in the message.

9.4 **Exemptions**

Interbank transfers and settlements where both the originator and beneficiary are banks or financial institutions would be exempted from the above requirements.

9.5 **Role of Ordering, Intermediary and Beneficiary banks**

(a) Ordering Bank

An ordering bank is the one that originates a wire transfer as per the order placed by its customer. The ordering bank must ensure that qualifying wire transfers contain complete originator information. The bank must also verify and preserve the information at least for a period of ten years.

(b) Intermediary bank

For both cross-border and domestic wire transfers, a bank processing an intermediary element of a chain of wire transfers must

ensure that all originator information accompanying a wire transfer is retained with the transfer. Where technical limitations prevent full originator information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record must be kept at least for ten years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

(c) Beneficiary bank

A beneficiary bank should have effective risk-based procedures in place to identify wire transfers lacking complete originator information. The lack of complete originator information may be considered as a factor in assessing whether a wire transfer or related transactions are suspicious and whether they should be reported to the Financial Intelligence Unit-India. The beneficiary bank should also take up the matter with the ordering bank if a transaction is not accompanied by detailed information of the fund remitter. If the ordering bank fails to furnish information on the remitter, the beneficiary bank should consider restricting or even terminating its business relationship with the ordering bank.

10 Combating Financing of Terrorism

10.1 In terms of PMLA Rules, suspicious transaction would include *inter alia* transactions which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Suitable mechanism shall be developed through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to the Financial Intelligence Unit – India (FIU-IND) on priority.

10.2 As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions, which is available in the Bank's Intranet. Further, the updated list of such individuals/entities can be accessed in the United Nations website at http://www.un.org/sc/committees/1267/consolist.shtml. Before opening any new account it shall be ensured that the name/s of the proposed customer does not appear in the list.

11 Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

i) The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities. In terms of Section 51A, 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 and 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.

ii) AML cell shall ensure that the procedure laid down in the UAPA Order dated August 27, 2009 (**Annexure V**) are strictly followed and shall ensure meticulous compliance to the Order issued by the Government.

iii) On receipt of the list of individuals and entities subject to UN sanctions from RBI, Bank shall ensure expeditious and effective implementation of the procedure prescribed under Section 51A of UAPA in regard to freezing/unfreezing of financial assets of the designated individuals/entities enlisted in the UNSCRs and especially, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts.

iv) In terms of Para 4 of the Order, in regard to funds, financial assets or economic resources or related services held in the form of bank

accounts, the RBI would forward the designated lists to the banks requiring them to:

a) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts with them.

b) In case, the particulars of any of the customers match with the particulars of designated individuals/entities, the Bank shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, held by such customer on their books to the 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 should necessarily be conveyed on e-mail :

c) Bank shall also send by post a copy of the communication mentioned in (b) above to the UAPA nodal officer of RBI, Chief General Manager, Department of Banking Operations and Development, Anti Money Laundering Division, World Trade Centre, Centre-1, 4th Floor, Cuffe Parade, Colaba, Mumbai –400005 and also by fax at No.022-22185792. The particulars apart from being sent by post/fax should necessarily be conveyed on e-mail :

d) Bank shall also send a copy of the communication mentioned in (b) above to the UAPA nodal officer of the

state/UT where the account is held as the case may be and to FIU-India.

e) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the Bank would prevent designated persons 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 should necessarily be conveyed on e-mail :

f) Bank shall also file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (b) above, carried through or attempted, as per the prescribed format.

v) **Freezing of financial assets**

a) On receipt of the particulars as mentioned in paragraph iv(b) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and /or the Central Agencies so as to ensure that the individuals/ entities identified by the Bank are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by Bank are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

b) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours

of such verification and conveyed electronically to the concerned Bank Branch under intimation to Reserve Bank of India and FIU-IND.

c) The order shall take place without prior notice to the designated individuals/entities.

vi) **Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.**

a) U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities.

b) To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

c) The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within five working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed

designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in RBI. The proposed designee, as mentioned above would be treated as designated individuals/entities.

d) Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to banks and the procedure as enumerated at paragraphs 2.13[(iii), (iv) and (v)] shall be followed.

e) The freezing orders shall take place without prior notice to the designated persons involved.

vii) Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank. The banks shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph (iv)(b) above within two working days. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days,

unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

viii) Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all banks through RBI.

12 Jurisdictions that do not or insufficiently apply the FATF Recommendations

12.1 Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account. In addition to FATF Statements circulated by Reserve Bank of India from time to time, (latest as on July 1, 2010, circular DBOD.AML.No. 16477/ 14.01.034/2009-10 dated March 26, 2010 issued by RBI), publicly available information for identifying countries, which do not or insufficiently apply the FATF recommendations shall be considered. It is clarified that special attention shall be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries that do not or insufficiently apply the FATF Recommendations and jurisdictions included in FATF Statements.

12.2 AML cell shall examine the background and purpose of transactions with persons (including legal persons and other financial institutions) from jurisdictions included in FATF Statements and countries that do not or insufficiently apply the FATF Recommendations. Further, if the transactions have no apparent economic or visible lawful purpose, the background and purpose of such transactions shall, as far as possible be examined, and written findings together with all documents should be retained and made available to Reserve Bank/other relevant authorities, on request.

13 Principal Officer

13.1 A Senior Management Officer of the Bank shall be designated as Principal Officer of the Bank and he / she shall be located at the head/corporate office of the Bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. Principal Officer will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The Principal Officer shall act independently and report directly to the senior management or to the Board of Directors.

13.2 Further, the role and responsibilities of the Principal Officer shall include overseeing and ensuring overall compliance with regulatory guidelines on KYC/AML/CFT issued from time to time and obligations under the Prevention of Money Laundering Act, 2002, rules and regulations made thereunder, as amended form time to time. The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency to FIU-IND.

13.3 With a view to enabling the Principal Officer to discharge his responsibilities effectively, the Principal Officer and other appropriate staff shall have timely access to customer identification data and other CDD information, transaction records and other relevant information.

14 Customer Education/Employee's Training/Employee's Hiring

14.1 Customer Education

Implementation of KYC procedures requires certain information from customers which may be of personal nature or which has hitherto never been called for. This can sometimes lead to a lot of questioning by the customer as to the motive and purpose of collecting such information. Hence specific literature/ pamphlets etc. shall be prepared to educate the customer of the objectives of the KYC programme. The front desk staff shall be specially trained to handle such situations while dealing with customers.

14.2 Employee's Training

An ongoing employee training programme shall be in place so that the members of the staff are adequately trained in KYC procedures. Training requirements should have different focuses for frontline staff, compliance staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind the KYC policies and implement them consistently.

14.3 Hiring of Employees

KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. Hence Bank shall put adequate screening mechanism in place as an integral part of its recruitment/hiring process of personnel.

15 POLICY UPDATES AND REVIEW

15.1 Updation or modification to the policy shall be initiated by Business Group as per business requirements keeping in view the RBI guidelines on KYC/AML or based on feedback / inputs received from branches, RPU /CPU. On recommendation of the Business Head, the same shall be put up for concurrence to the Standing Committee on KYC and AML.

15.2 The modifications / updates to the policy may also be initiated by Principal Officer based on the analysis of transactions monitored in customer accounts / operational risk events. The same shall be put up for approval to the Standing Committee on KYC and AML.

15.3 The policy shall be put up for review to the Board of Directors once a year by the Principal officer.

ANNEXURE - I

RISK CATEGORISATION OF CUSTOMERS

Types of customers and their risk categorization -

High Risk Customers

1. Individuals and entities in various United Nations Security council Resolutions (UNSCRs) such as UN 1267 etc.
2. Individuals or entities listed in the schedule to the order under section 51 A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of and for coping with terrorist activities.
3. Individuals and entities in watch lists issued by Interpol and other similar international organizations.
4. Customers with dubious reputation as per public information available or commercially available watch lists.
5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk.
6. Customers conducting their business relationship or transaction 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 in various geographic locations etc.
7. Customers based in high risk countries/jurisdictions or locations.
8. Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner;
9. Non-resident customers and foreign nationals
10. Embassies/ Consulates
11. Off-shore (foreign) corporation/business
12. Non face-to-face customers
13. High net worth individuals
14. Partnership Firms
15. Firms with 'sleeping partners'
16. Walk-in-Customers
17. Companies having close family shareholding or beneficial ownership
18. Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
19. Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence.
20. Investment Management / Money Management Company/ Personal Investment Company

21. 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 financial institution.
22. Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc
23. Trusts, charities, NGO's/NPOs (those operating on a "cross-border' basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
24. Money service Business: including seller of: Orders/ Travelers Checks / Money Transmission /Check Cashing / Dealing or Exchange
25. Business accepting third party cheque (except supermarkets or retail stores that accept payroll cheque / cash payroll cheque)
26. Gambling/gaming including "junket Operators" arranging gambling tours
27. Dealers in high value or precious goods(e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses, estate agents and real estate brokers).
28. Customers engaged in a business which is associated with higher levels of corruption (e.g. arms manufacturers, dealers and intermediaries)
29. Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
30. Customers that may appear to be Multi level marketing companies etc.

Medium Risk Customers

1. Non Bank Financial Institution
2. Stock brokerage
3. Import/ Export
4. Gas Station
5. Car/ Boat/ Plane Dealership
6. Electronics (wholesale)
7. Travel agency
8. Used car sales
9. Telemarketers
10. Providers of telecommunications service, internet café, IDD call service, phone cards, phone center.
11. Dot-com company or internet business
12. Pawnshops
13. Auctioneers
14. Cash-intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
15. Sole Practitioners or Law firms (small, little known)
16. Notaries (small, little known)
17. Secretarial (small, little known)
18. Accountants (small, little known)
19. Venture capital companies

Low Risk Customers

1. Individuals (Other than included in High and Medium Risk categories above)
2. Government departments and Government owned Companies, regulatory and statutory bodies
3. Non Profit Organisations / Non Government Organisations promoted by United Nations or its agencies
4. All other categories of accounts / customer not falling under the above indicated High and Medium Risk classifications.

Annexure – II

Information to be obtained from customer for creating customer profile

The following information shall be obtained from the customer at the time of account opening for profiling customers based on perceived risk.

	Customer Type	Information to be obtained from customer
1	Individuals	▪ Profession – Salaried / Self-employed. ▪ Annual Income ▪ If self-employed, nature of profession / business ▪ Annual turnover in case self-employed supported by IT returns ▪ PAN number
2	Sole Proprietorship	▪ Name of sole proprietor ▪ Type of business ▪ Annual turnover supported by IT returns ▪ Name and address of clients (Supplier & Purchaser)
3	Partnership	▪ Name of partners ▪ Type of business ▪ Annual turnover supported by IT returns ▪ Name and address of clients (Supplier & Purchaser)
4	Companies	▪ Name of directors ▪ Type of business ▪ Annual turnover supported by Annual Report ▪ Name and address of clients (Supplier & Purchaser)
5	Trust, Association, Society, Club (TASC)	▪ Names and addresses of trustees ▪ Purpose of the TASC ▪ Last year's total income supported by IT returns

ANNEXURE III

Customer Identification Procedure

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Given below is the indicative procedure which may be reviewed and implemented by the Standing Committee on KYC / AML from time to time.

1. **Customer Identification** –

   The identification procedure of Bank for a new customer is described below:

   i) Completed account opening form AND

   ii) Self-signed cheque or Cash deposited personally by the customer at the Branch to be certified by Branch Head AND

   iii) Identity, Signature & Address (ISA) documentation check OR

   Introduction by an existing customer of the Branch having a banking relationship of 6 months or more and having satisfactory conduct of account alongwith the Address proof OR

   Introduction by an existing Banker (Signature Verification report from existing Bank will be required) alongwith the Address proof

2. Identity, Signature and Address (ISA) Document Check

The following documents listed below are required for ISA check :

i) Completed account opening form AND

ii) Self-signed cheque or Cash deposited personally by the customer at the branch AND

iii) Passport copy OR

iv) In case Passport is not available, copy of one document each from List A and List B (Address proof documents) is required. The following table gives the document wise checks.

LIST A – DOCUMENTS FOR ISA CHECK

Documents	**Identity check**	*Signature check*	**Address check**
i) PAN Card	Yes	Yes	No
ii) Voter's ID card * (to be accepted with a self-signed cheque)	Yes	No	Yes
iii) Driving license (to be accepted with a self-signed cheque)	Yes	No	Yes
iv) Defense ID/Govt. ID/Indian post ID	Yes	Yes	No
v) Employees ID Card **(for Corporate Salary Accounts)** In the case of payroll accounts: If EMPLOYEE ID card is not there then 'letter of Introduction' from HR dept or any authorized Signatory to sign on Company letter head – certifying Identity and signature. However Bank has to be aware about the competent authority designated by the concerned employer to issue such letter / certificate. This will be done on each AoF for signature verification. In case of mailing address being different from the corporate address then any address proof document to be taken. In addition to the certificate from employer, at least one of the officially valid identity proof as mentioned above should be obtained. vi) In the case of Defense accounts, Defense ID cards are not permitted to be given for ISA. Hence in these accounts only a letter from the commanding officer of the regiment to be taken certifying ISA.	Yes	Yes	No
vii) Photo Credit Card	Yes	Yes	No

LIST B – DOCUMENTS FOR ADDRESS CHECK

Documents		Identity check	*Signature* check	Address check
i)	Latest existing Bank account statement or Bank passbook, where address is mentioned	No	No	Yes
ii)	Ration Card	No	No	Yes
iii)	Latest Credit Card statement	No	No	Yes
iv)	Latest Electricity Bill	No	No	Yes
v)	Latest Telephone Bill	No	No	Yes
vi)	Latest Copy of LIC or Insurance Premium receipt	No	No	Yes
vii)	Letter from employer certifying the current mailing address only from private limited and public limited companies	No	No	Yes
viii)	Existing valid house registered lease agreement on stamp paper(in case of rented / leased accommodation or shifting / transfer of residence)	No	No	Yes

The validity of the documents given in List B above should not be more than 3 months.

3. Customer Identification Documents (<u>Indicative</u>) –

The following table provides the different types of accounts and documents to be obtained from customers along with the Account Opening Form duly filled in and signed along with recent colour photograph(s) of the customer(s) and initial deposit.

Features	**Documents**
1. Accounts of individuals / HUF - Legal Name or any other name used	Anyone of (i) Passport (valid) (ii) PAN card (iii) Voter's Identity Card (iv) Driving license (valid) (v) Indian Post ID (vi) Government Identity card (subject to the bank's satisfaction) (vii) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of the Bank (viii) Employee ID Card (in case of corporate salary accounts only) with one more identity proof (ix) Photo Debit / Credit card (valid) (x) Other Bank's signature verification (xi) HUF declaration signed by Karta and Major coparceners including details of minor coparceners along with date of birth (xii) Marriage Ceritficate / Nikahnama for Women (alongwith identity document in Maiden name and valid address proof of the spouse) (xiii) Defense Dependent's Card (xiv) Defense Ex-Service Man Card issued to defense employees (xv) Citizenship Card issued in North Eastern States for ISA, if these details are available in the card. Or Introduction by existing customer who is an account holder with IDBI Bank for more than 6 months with satisfactory conduct of account.
Correct permanent address	(i) Telephone bill in the name of the customer (ii) Bank account statement or passbook (iii) Letter from any recognized public authority

	(iv) Electricity bill (v) Ration card (vi) Municipal Corporation Bill (vii) Letter from employer only public and private limited companies (subject to satisfaction of the Bank) (viii) Existing house registered lease agreement on stamp paper (in case of rented / leased accommodation or shifting / transfer of residence only) (In case of Corporate salary accounts notarized lease agreement is allowed) (Anyone document which provides customer information to the satisfaction of the bank will suffice). List of documents that can be taken as ISA (Identity, Signature and Address) proof are mentioned in LIST A & LIST B.

Additional documents to be taken for the following individual accounts are given below :

Feature	**Documents to be taken**
2. *Minor Accounts*	Copy of any one of the following : (i) Birth Certificate issued by Municipal authorities (ii) Passport (iii) Pan Card (iv) 10th or 12th Mark Sheet (v) Bonafide school leaving certificate confirming the age of Minor (vi) Report card signed by Class Teacher / Principal / Vice-Principal showing date of birth. (vii) School ID card with Photo and Date of Birth mentioned duly signed by school authorities (Principal / Vice-Principal). (viii) Letter from College/School/University attesting the identity and signature (letter should have the photograph of student with his signature) (ix) Letter from College/School/University confirming the address as per their record
3. Non-Resident Indian (NRI) Customers	Copy of : (i) Valid Passport & Valid Resident / Employment Visa for NRI / NRO Accounts. **In case account opened in person:**

	1.Valid Passport with overseas resident address or work permit (i.e. Green Card as residence permit for USA, H1 Visa as work permit for USA or Honk Kong ID card for residence of Hongkong) 2. If the visa is not stamped in the passport (as is the case with some of the european countries) copy of the resident permit issued by their immigration authorities 3. Separate proof of Non Resident status if the passport holds Indian Address and resident Visa permit is not included in passport. 4. PIO (person of Indian origin) Card issued by the Government of India in case of foreign passport. If PIO card is not available, self declaration by the customer. 5. In case the Indian nationality / origin cannot be ascertained based on the documents submitted, a self declaration giving details of the Indian Origin confirming the city and state of birth in India. 6. Photograph of individual account holder. **For persons employed with foreign shipping company:** a. Initial work contract b. Last wage slip c. CDC (Continuous Discharge Certificate) d. Employment contract / letter on the letter head of the agent wherein, the overseas address of the shipping co / airline is prominently displayed. **For contract employees:** 1. Last work contract 2. Letter from local agent confirming next date of joining the foreign vessel (not more than six months of date of last return to India) 3. Principal's overseas address or current work contract. **In case of documents sent by mail:** All document / signatures to be attested by any one of the following: 1.Indian embassy 2.Overseas Notary

	3. Local banker of the NRI
4. Senior Citizens	Copy of : i) Passport ii) Driving License iii) Ration Card iv) Pension Card v) Government ID Card vi) School Leaving Certificate vii) Life Insurance Policy viii) Birth Certificate

Feature	Documents to be taken
5. Accounts of companies - Name of the company - Principal place of business - Mailing address of the company - Telephone/ Fax Number	(i) Certified true copy of Certificate of incorporation and (ii) Certified true copy of Memorandum of Association and (iii) Certified true copy of Articles of Association and (iv) Certified true copy of Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account. Resolution to be certified by Company secretary and One director who has attended the said meeting. and (v) Power of Attorney granted to its managers, officers or employees to transact business on its behalf. and (vi) Copy of PAN Card. (vii) Copy of telephone bill confirming the address of the company (viii) Certified true copy of commencement of business (ix) In case of change in directors - Form 32 issued by Registrars of Companies (ROC) showing the new directors along with the receipt of confirmation of submission to ROC (mandatory). Or latest annual returns where the directors names are listed and filed with ROC. (x) In case of change in the registered address of the company – Form 18 issued by ROC along with receipt of submission to ROC (mandatory). (xi) Passport size photographs of directors / authorised signatories and (xii) Complete address of the directors / authorised signatories (xiii) Documents for Identity and Signature check of the authorised signatories / directors (any one from List A and List B) (xiv) NOC from the Lending Banker if customer enjoys Credit facilities. (xv) Existing Bank statement from current banker (xvi) Introduction by Existing Current Account holder who is holding an account with IDBI Bank for more than 6 months & with satisfactory conduct of account.

Feature	**Documents to be taken**
6. Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Entity proof of the firm (any one of the following) and a. Shops & Establishment Certificate b. Municipal License c. Chartered Accountant certificate in case of partnership firm d. Latest IT returns filed in name of the firm e. Existing Current account bank statement in the name of the firm. f. District Industries Certificate confirming registration of SSI (ii) Registration certificate if registered and (iii) Partnership deed (duly certified true copy) and (iv) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (new RBI) (v) Any officially valid document (documents specified for identity and signature checks as per List A & List B for this purpose) identifying the partners and the persons holding the Power of Attorney and their addresses. (vi) Telephone bill in the name of firm/partners. (vii) PAN Card (viii) NOC from the Lending Banker if customer enjoys Credit facilities. Introduction by Existing Current Account holder who is holding an account with IDBI Bank for more than 6 months and with satisfactory conduct of account. HUFs can be partners in Current or Fixed Deposits, however no overdraft to be allowed.

7. Accounts of trusts & foundations - Names of trustees, settlers, beneficiaries, signatories - Names and addresses of the founder, the managers / directors and beneficiaries - Telephone/ fax numbers	(i) Certificate of registration, if registered (ii) Certified True copy of the Trust Deed. (iii) POA granted to transact business on its behalf (iv) Any officially valid document (documents specified for identity and signature checks as per List A & List B for this purpose) to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders / managers / directors and their addresses. (v) Resolution of the managing body of trust / foundation (vi) Copy of Bye-laws (vii) Telephone bill confirming address of the trust / foundation (viii) Passport size photo of trustees / authorised seniorities (ix) Documents for ISA check of the authorised signatories (x) IT Exemption letter (for charitable institutions) (xi) PAN (xii) NOC from the Lending Banker if customer enjoys Credit facilities ISA check of Trustees is not necessary. ISA check is required for all authorized signatories.

	Documents to be taken
8. Accounts of Societies, Clubs & Associations - Names of Authorised Signatories - Names and addresses of the founder, the managers/ directors and the beneficiaries - Telephone/fax numbers	(i) Certificate of registration, if registered (ii) Certified True copy of the Byelaws (iii) Power of Attorney granted to transact business on its behalf (iv) Any officially valid document to identify the Signatories, and those holding Power of Attorney, founders/managers/ directors and their addresses (v) Resolution of the managing body of the Societies / Club / Association (vi) Telephone bill confirming address (vii) PAN Card (viii) NOC from the Lending Banker if customer enjoys Credit facilities
9. Power of Attorney (POA) Holder / Mandate Holder	(i) Mandate letter signed by the all customers along with the signature of Mandate holder. (ii) For POA, duly certified POA agreement along with the signatures of both customer & POA holder. (iii) Identity document of the Mandate / POA Holder (iv) Photograph of Mandate / POA holder .
10. Sole Proprietorship Accounts - Proof of the name of address and activity of the concern	(i) Proprietor's complete Identification, Signature and Mailing Address proof documents along with Telephone Number confirmation, (ii) Existing current account Bank statement in the same name of the firm) confirming existence of the Firm, (iii) Telephone bill confirming address (iv) NOC from the Lending Banker if customer enjoys Credit facilities (v) PAN card with mailing address proof if the initial deposit is in cash. (vi) Introduction by Existing Current Account holder who is holding an account with IDBI Bank for more than 6 months and with satisfactory conduct. (vii) <u>Any Two proofs from the below for identity</u> - (i) Registration certificate/licence issued by Municipal authorities such as Shop & Establishment certificate / Trade Licence. (ii) CST / VAT /Service Tax Certificate or letter of registration for CST / VAT /Service Tax.

	(iii) Certificate/Registration document issued by Service Tax/Professional Tax authorities. (iv) Registration certificate (in the case of a registered concern) (v) IEC (Importer Exporter Code) issued by DGFT (vi) Certificate / Registration documents issued by Sales Tax / Service Tax / Professional Tax authorities. (vii) License issued by the registering authority like certificate of practice issued by Institute of Chartered Accountant of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, etc. (viii) Licence issued by Explosives Rules. (ix) Certificate of registration under any specific Statute / Act of the government. (x) IRDA (Insurance Regulatory and Development Authority) licence in the name of the entity with address mentioned. (xi) Valid Business Licence or certificate of registration issued by State / Central government authority (Validity would include the grace period for renewal as mentioned in the certificate). (xii) Permission Issued by respective government authority for units in SEZ (Special Economic Zone), STP (Software Technology Park), EOU (Export Oriented Unit), EHTP (Electronic Hardware Technology Park), DTA (Domestic Tariff Area) and EPZ (Export Processing Zone) in the name of the entity mentioning the address allotted. (xiii) Registration certificate of recognized Provident Fund with PF commissioner. (xiv) Factory Registration certificate issued by any state / central government authority. (xv) RBI/SEBI Registration Certificate. (xvi) Licence to sell stock or exhibit for Sale or distribute Insecticides, under the Insecticides Rules, issued by respective state /union government department. (xvii) Permission issued by village Administrative Officer / Panchayat Head / Mukhiya / Village Developmental officer / Block development officer or Equal Rank officer for customers in rural / village areas and President/CEO if document issued by Nagar Parishad / Zilla Parishad. (xviii) Letter/ Certificate/ NOC issued by village

	Administrative Officer / Panchayat Head / Mukhiya / Village Developmental Officer / Block Development Officer or Equal Rank officer for customers in rural / village areas and President/CEO if document issued by Nagar Parishad / Zilla Parishad stating the details of existence of the firm may be accepted. In such cases, (wherever permission is not available), CPV by a bank staff shall be mandatory. (xix) Registration Certificate issued by District Industries Center for firm registered as SSI/Micro/Medium Unit. (xx) Licence issued under Contract Labour (Regular & Abolition) Act 1970. (xxi) Licence issued by police department under the provisions of State Police Acts. (xxii) Latest Income Tax Return filed in name of proprietor, provided the name of firm shall reflect on the ITR 4 Form filed. The name generally appears on page –2. (xxiii) Acknowledgment of ITR 4 return may be accepted provided the name of the firm is mentioned on the acknowledgment. (xxiv) Latest Sales Tax Returns filed in name of firm (CST/VAT/Service Tax/Profession Tax) duly acknowledged. (xxv) TAN Allotment Letter in name of firm only. The same shall not be acceptable if issued in the name of the proprietor. Print out of online TAN registration details shall also be accepted. (xxvi) Latest available Income Tax Wealth Tax Assessment order along with print out from PAN website confirming the PAN number & name of entity. (xxvii) Latest property tax / Water tax bill / Utility bill or receipt in the name of the firm issued by local government authorities or the service provider. In case of telephone bill the bill needs to be for a landline connection. (xxviii) Certificate issued by the Chartered Accountant confirming existence of the firm. The name of the Chartered Accountant would need to be validated from the Chartered Accountants directory. This would need to be accompanied by a site visit conducted by a permanent bank staff. (xxix) Registration Certificate / Licence issued by

	Rubber Board / Spices Board / Tea Board / Coffee Board / Coir Board / Tobacco Board / Notional Jute Board / Pollution Control Board. (xxx) Licence issued by Agriculture Produce Marketing Committees (APMC) / Gramin Mandis / KVIC. (Any two of the above documents would suffice. These documents should be in the name of proprietary concern)

Feature	Documents to be taken
11. Government Accounts	A.) Accounts of Executive Engineers / SDO (Assistant Engineer) / BDPO (Block Development & Panchayat Officers / DDPO (Dist. Development & Panchayat Officer): 1. General circular from the concerned dept. within the respective state/province stating that the above office / official is authorized to function as DDO (drawing & disbursal officer), And 2. Letter of Intent signed by Executive Engineer / SDO / BDPO / DDPO to open an account with IDBI Bank or The immediate officer (reporting authority) would issue a letter confirming that an official is authorized to open and operate the account, And 3. Letter of Intent signed by Executive Engineer / SDO / BDPO / DDPO to open an account with IDBI Bank B) Accounts of SDM / Deputy Commissioner: - <u>Account in the name of SDM or Deputy Commissioner:</u> Account necessarily to be in the name of SDM or Deputy Commissioner of the sub division or city as the case may be. 1. Letter of Intent signed by SDM / DC to open an account with IDBI Bank, And 2. Government order / circular confirming the name and designation of SDM / DC. <u>C) Account in the name of Estate Officer:</u> If SDM and DC hold charge of the Estate Office, then 1. Letter of Intent signed by SDM / DC to open an account with IDBI Bank, And 2. Letter confirming that the Deputy Commissioner works as the Estate Officer, And 3. A copy of a circular / order confirming the same that 'Mr. XYZ transferred as DC cum Estate officer of the city / or SDM cum Estate Officer of the city..." Additionally (not mandatory) 1. ISA of authorized signatories 2. Self-signed Cheque All accounts need to be signed by Branch Head confirming that they have met the concerned officials.

Annexure – IV

Name of Financial Institution:

QUESTIONNAIRE ON

KNOW-YOUR CUSTOMER / ANTI MONEY LAUNDERING / COMBATING FINANCING OF TERRORISM

Information submitted to: IDBI Bank Ltd

I	**General Information**	
a.	Name of your organisation:	
b.	Bank Licenses No. & Date:	
c.	License Issuing Authority:	
d.	Address:	
e.	Registered Office at:	
f.	Head Office at:	
g.	Principal Operating Office at:	
h.	E-Mail:	
i.	Website:	
j.	Name of Anti Money Laundering Officer / Principal Officer with Telephone No, FAX, E-Mail:	
k.	Name of the Supervisory Organisation in your Country	
l.	If FI is publicly traded, name of Exchanges:	

II.	General KYC/AML/CFT Policies, Practices and Procedures:	Yes	No
1.	Has the country in which you are located established laws designed to prevent money laundering? If yes, is your institution subject to such laws?		
2.	Does your institution maintain a physical presence in the licensing country? Physical presence means a place of business located at affixed address (other than solely an electronic address, a post office address or an accommodation address) and in a country in which bank employees one or more individuals full time and maintains operating records related to banking activities and where the bank is subject to inspection by the banking authority which licensed the bank to conduct banking activities.		
3.	Does the FI have a legal and regulatory compliance program that includes a designated compliance officer who is responsible for coordinating and overseeing the AML program, on a day-to-day basis, which has been approved by Senior Management of the FI?		
4	Does the law require banks to have procedures for the prevention of money laundering?		
5	Has your institution developed written policies documenting the processes that they have in place to prevent, detect and report suspicious transactions that has been approved by senior management/Board of FIs? IF YES, ESTABLISHED DATE: REVIEWED DATE:		
6	In addition to inspections by the government supervisors/regulators, does the FI client have an internal audit function or other independent third party that assesses AML policies and practices on a regular basis?		
7	Does your institution have a policy prohibiting accounts/relationships with shell banks? (A Shell bank is defined as a bank incorporated in a jurisdiction in which it has no physical presence and which is unaffiliated with a regulated financial group)		
8	Does your institution have a policies covering relationships with politically exposed persons consistent with industry best practices?		
9	Does the FI have appropriate record retention procedures pursuant to applicable law? IF YOUR ANSWER IS YES, FOR HOW LONG :		
10	Does your institution require that its AML policies and practices be applied to all branches and subsidiaries of the financial institution in the home country and in locations outside of home country?		
11	Does your country adhere to the 40 Anti Money Laundering recommendations and 9 Special terrorist financing recommendations developed by the Financial Action Task Force (FATF)? If your country is not a member of the FATF, please provide the name of the comparable organisation to which your		

	country belongs, e.g. the name of the FATF-style regional body to which your country belongs, e.g. the name of the FATF-style regional body to which your country belongs? (APG-Asia Pacific Group on Money Laundering, MONEYVAL, etc.)		
12	Do the laws and regulations in your country prohibit your institution from opening an anonymous account?		
13	Has your Institution had any regulatory or criminal enforcement action resulting from violation of AML laws or regulations		

III	**Risk Management**		
1	Does the FI have a risk-focused assessment of its customer base and transactions of its customers?		
2	Does your institution determine the appropriate level of enhanced due diligence necessary for those categories of customers and transactions that the institution has reason to believe pose a heightened risk of illicit activities at or through the institution?		
3	Whether proper system is put in place to track transactions on the basis of risk classification of countries and you do not entertain transactions with High Risk Categorised Countries?		

IV	Know Your Customer, Due Diligence and Enhanced Due Diligence		
1	Has your institution implemented systems for identification of its clients, including client information in case of recorded transactions, account opening such as family name/ name of firm, activities/job, nationality, street address, telephone number, country/state that issued it?		
2	Does your institution have procedures to establish a record for each client noting their respective identification documents and know your client information collected at account opening? Are copies of identification documents retained in your possession for reference? If so, how long are the records retained?		
3	Does the FI collect information and access its FI customer's AML policies or practices?		
4	Does your institution take steps to understand the normal and expected transactions of its customer's base on its risk assessment of its customers?		

V	**Reportable transactions and prevention and detection of transactions with illegally obtained funds**		
1	Does your institution have policies for the identification and reporting of transactions that are required to be reported to the authorities?		
2	Does your institution screen transactions for clients or transactions the financial institutions deems to be of significantly high risk that special attention to such customer or transactions is necessary prior to completing any such transactions?		
3	Does your institution have procedures to identify transaction structured to avoid large cash reporting requirements?		
4	Does your institution have policies to reasonably ensure that it only operates with correspondent banks that possess licenses to work in their countries of origin?		
5	Is your institution subject to regulatory requirements on reporting of suspicious activities? Which authority is in charge of receiving suspicious activities report?		

VI	**Transaction Monitoring**		
1	Does the FI have a monitoring program for suspicious or unusual activity that covers funds transfers and monetary instruments (such as traveler's cheques, money orders, etc)?		
2	Is your institution subject to regulatory laws for retention of records of Suspicious Transaction Reports? If so for how long?		
3	Within last one year has your institution reported to the regulatory authority any case of money laundering or financing of terrorism?		

VII	**AML Training**		
1	Does your institution provide AML training to relevant employees that include identification and reporting of transactions that must be reported to govt. authorities, examples of different forms of money laundering involving the bank products and services and internal policies to prevent money laundering?		
2	Does the FI retained records of its training sessions including attendance records and relevant training material used?		
3	Does your institution communicate new AML related laws or changes to existing AML related policies or practices to relevant employees?		
4	Does your institution have an established audit and compliance review function to test the adequacy of AML and terrorist financing procedures?		

5	Does the FI employ agents to carry out some of the functions of the FI and if so does the FI provide AML training to relevant agents that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving the DI's products and services and internal policies to prevent money laundering?		

VIII	**Documents to be enclosed in support:**		
a.	Bank Licence		
b.	Memorandum of Association		
c.	Articles of Association		
d.	KYC / AML Policy		
e.	List of Shareholders with percentage		
f.	List of Directors		
g.	List of Top Management Officials		

(Signature)
Money Laundering Reporting Officer / The Principal Officer:
Name of The Principal Officer (MLRO)
Financial Institution Name:
Location:
Telephone Number:
Fax Number:
E-Mail:
Date:

Annexure - V

File No.17015/10/2002-IS-VI
Government of India
Ministry of Home Affairs
Internal Security-I Division
*****

New Delhi, dated 27th August, 2009

ORDER

Subject : Procedure for implementation of Section 51A of the Unlawful Activities (Prevention)Act, 1967

The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act.
Section 51A reads as under:-

"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to –

(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",

The Unlawful Activities (Prevention) Act define "Order" as under:-

"Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.
In order to expeditiously and effectively implement the provisions of Section 51A, the following procedures shall be followed:-

Appointment and Communication of details of UAPA nodal officers

2. As regards appointment and communication of details of UAPA nodal officers –

(i) The UAPA nodal officer for IS-I division would be the Joint Secretary (IS.I), inistry of Home Affairs. His contact details are 011- 23092736(Tel), 011-23092569(Fax) and (e-mail).
(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA nodal officer and communicate the name and contact details to the IS-I Division in MHA.
(iii) The States and UTs should appoint a UAPA nodal officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the IS-I Division in MHA.

(iv) The IS-I Division in MHA would maintain the consolidated list of all UAPA nodal officers and forward the list to all other UAPA nodal officers.

(v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA nodal officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(vi) The consolidated list of the UAPA nodal officers should be circulated to the nodal officer of IS-I Division of MHA in July every year and on every change. Joint Secretary(IS-I), being the nodal officer of ISI Division of MHA, shall cause the amended list of UAPA nodal officers to be circulated to the nodal officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals/entities

3. As regards communication of the list of designated individuals/entities-

(i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, IS-I Division and Foreigners' Division in MHA.

(ii) The Regulators would forward the list mentioned in (i) above (referred to as designated lists) to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively.

(iii) The IS-I Division of MHA would forward the designated lists to the UAPA nodal officer of all States and UTs.

(iv) The Foreigners Division of MHA would forward the designated lists to the immigration authorities and security agencies.

Regarding funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc.

4. As regards funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc., the Regulators would forward the designated lists to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. The RBI, SEBI and IRDA would issue necessary guidelines to banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies requiring them to –

(i) Maintain updated designated lists in electronic form and run a check on the given parameters on a regular basis to verify whether individuals or entities listed in the schedule to the Order (referred to as designated individuals/entities) are holding any funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. with them.

(ii) In case, the particulars of any of their customers match with the particulars of designated individuals/entities, the banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, stocks or insurance policies etc. held by such customer on their books to the 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 should necessarily be conveyed on e-mail .

(iii) The banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU0IND, as the case may be.
(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt**,** the banks stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons 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 should necessarily be conveyed on e-mail:
(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above , carried through or attempted, as per the prescribed format.

5. On receipt of the particulars referred to in paragraph 3(ii) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and/or the Central Agencies so as to ensure that the individuals/entities identified by the banks, stock exchanges/depositories, intermediaries regulated by SEBI and Insurance Companies are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services, reported by banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies are held by the designated individuals/entities. This verification would be completed within a period not exceeding 5 working days from the date of receipt of such particulars.

6. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy thereof to all the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic assets or economic resources or related services available for the benefit of the designated individuals/entities or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy of the order under Section 51A, to all Directors General of Police/Commissioners of Police of all states/UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act. The order shall take place without prior notice to the designated individuals/entities.

Regarding financial assets or economic resources of the nature of immovable properties.

7. IS-I Division of MHA would electronically forward the designated lists to the UAPA nodal officer of all States and UTs with the request to have the names of the designated individuals/entities, on the given parameters, verified from the records of the office of the Registrar performing the work of registration of immovable properties in their respective jurisdiction.

8. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA nodal officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Joint Secretary (IS.I), Ministry of Home Affairs, immediately within 24 hours at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail:

9. The UAPA nodal officer of the State/UT may cause such inquiry to be conducted by the State Police so as to ensure that the particulars sent by the Registrar performing the work of registering immovable properties are indeed of these designated individuals/entities. This verification would be completed within a maximum of 5 working days and should be conveyed within 24 hours of the verification, if it matches with the particulars of the designated individual/entity to Joint Secretary(IS-I), Ministry of Home Affairs at the Fax telephone numbers and also on the e-mail id given below.

10. A copy of this reference should be sent to the 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 would necessarily be conveyed on e-mail: MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the State/UT. The order shall take place without prior notice, to the designated individuals/entities.

12. Further, the UAPA nodal officer of the State/UT shall cause to monitor the transactions/accounts of the designated individual/entity so as to 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. The UAPA nodal officer of the State/UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and

associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

14. To give effect to the requests of foreign countries under U.N. Security Council Resolution 1373, the Ministry of External Affairs shall examine the requests made by the foreign countries and forward it electronically, with their comments, to the UAPA nodal officer for IS-I Division for freezing of funds or other assets.

15. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in Regulators. FIU-IND and to the nodal officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities.

16. Upon receipt of the requests by these nodal officers from the UAPA nodal officer of IS-I Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

The freezing orders shall take place without prior notice to the designated persons involved.

Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person

17. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers.

18. The banks stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph 4(ii) above within two working days.

19. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within 15 working days, unfreezing the funds, financial assets or economic resources or related services,

owned/held by such applicant under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States/UTs. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, relating to funds, financial assets or economic resources or related services, would be communicated to all banks, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the State/UT nodal officer by IS-I Division of MHA.

Regarding prevention of entry into or transit through India

21. As regards prevention of entry into or transit through India of the designated individuals, the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities.

22. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

Procedure for communication of compliance of action taken under Section 51A.

23. The nodal officers of IS-I Division and Foreigners Division of MHA shall furnish the details of funds, financial assets or economic resources or related services of designated individuals/entities frozen by an order, and details of the individuals whose entry into India or transit through India was prevented, respectively, to the Ministry of External Affairs for onward communication to the United Nations.

24. All concerned are requested to ensure strict compliance of this order.

(D .Diptivilasa)
Joint Secretary to Government of India