



# **The Jind Central Cooperative Bank Limited Jind**

**KYC/ AML/ CFT Policy  
(Amendment) - 2017**

# INDEX

S. No.	Topic	Page No.
1.	Preamble	2
2.	Objective, Scope & Application	2
3.	Definition of Money laundering	4
4.	Key elements of Policy	7
5.	Obligation under Money Laundering Act, 2002	7
6.	Customer Acceptance Policy	8
7.	Customer Identification Procedure	11
8.	Monitoring and reporting of transaction	14
9.	Risk Management	16
10.	Customer Education	16
11.	Employee Training	17
12.	Recruitment/ Hiring of Employees	18
13.	Internal Control and System	18
14.	Evaluation of KYC by Internal Audit and Inspection Section	19
15.	Duties and Responsibilities	19
16.	Some special cases	19
17.	CFT (Combating Finance to Terrorism)	19
18.	Freezing of assets under section 51 of Unlawful Activities (Prevention) Act 1967	20
19.	Glossary	26
20.	CIP (Annexure-I)	27
21.	Risk Category of assets (Annexure-II)	29-30
22.	CIP Details (Annexure-III)	31-39
23.	Customer Behavioural Indicators (Annexure-IV)	40
24.	An indicator list of suspicious activities (Annexure-V)	41
25.	Duties & Responsibilities and Accountability (Annexure-VI)	45
26.	Questionnaire (Annexure-VII)	46

## 1. Preamble

The Jind Central Cooperative Bank Limited Jind is committed to adherence of KYC standards, AML and CFT for which Reserve Bank of India and NABARD have been issuing guidelines

The guidelines incorporate the:

- Obligations on bank under the Prevention of Money Laundering Act (**PMLA**), 2002.
- Recommendations made by the Financial Action Task Force(**FATF**) on AML Standards and CFT
- Paper issued on Customer Due Diligence(**CDD**) for banks by the Basel Committee on Banking Supervision.

The Jind Central Cooperative Bank Limited Jind hence frame and put in place a comprehensive policy, duly approved by the Board of Directors, in this regard. This policy document has been prepared in line with the RBI/NABARD guidelines and incorporates the Bank's approach to **KYC, AML** and **CFT** issues, however in case of contradiction and ambiguity the RBI/ NABARD guidelines may always be referred in this regard.

## 2. Objectives, Scope and Application of the Policy:

The primary objective of the Policy is to prevent The Jind Central Co-operative Bank Ltd. Jind from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. Purposes proposed to be served by the Policy are:

- (i) To prevent criminal elements from using The Jind Central Cooperative Bank Limited Jind for money laundering activities.
- (ii) To enable The Jind Central Cooperative Bank Limited Jind to know/understand the customers and their financial dealings better which, in turn, would help the bank to manage risks prudently.
- (iii) To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/laid down procedures.
- (iv) To comply with applicable law and regulatory guidelines.
- (v) To ensure that the concerned staff are adequately trained in KYC/AML/CFT procedures.
- (vi) The Bank will initiate steps to create awareness and give wider publicity by circulating the poster and booklet amongst all their branches and to the customers / general public and display the poster prominently in their premises.

This Policy is applicable to all branches/offices of The Jind Central Cooperative Bank Limited Jind and is to be read in conjunction with related operational guidelines issued from time to time.

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

### **3. Definition:**

#### **3.1 Customer:**

For the purpose of 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.}
- Beneficiary 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 financial transactions which can significance reputational or other risks to the Bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

#### **3.2 Money Laundering:**

**Section 3 of PMLA has defined the “offence of money laundering” as under:**

“Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party processor activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money laundering”.

Money launderers use the banking system for cleansing ‘dirty money’ obtained from criminal activities with the objective of hiding/disguising its source. The process of money laundering involves creating a web of financial transactions so as to hide the origin and true nature of these funds.

For the purpose of this document, the term money laundering would also cover financial transactions where the end use of funds goes for terrorist financing irrespective of the source of the funds.

#### **3.3 Customer Due Diligence:**

Customer Due Diligence (CDD) can be defined as any measure undertaken by a financial institution to collect and verify information and positively establish the identity of a customer. The base of CDD would be the board approved Customer Acceptance Policy of a bank. Based on Customer Acceptance Policy, the Customer Identification Procedures needs to be drawn.

#### **3.4 Designated Director:**

Designated Director" means a person designated by the reporting entity to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules and includes --

- (i) The Managing Director or a whole-time Director duly authorized by the Board of Directors if the reporting entity is a company,
- (ii) The managing partner if the reporting entity is a partnership firm,

- (iii) The proprietor if the reporting entity is a proprietorship concern,
- (iv) The managing trustee if the reporting entity is a trust,
- (v) A person or individual, as the case may be, who controls and manages the affairs of the reporting entity if the reporting entity is an unincorporated association or a body of individuals, and
- (vi) Such other person or class of persons as may be notified by the Government if the reporting entity does not fall in any of the categories above.

Explanation. - For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 1956 (1 of 1956).<sup>2</sup>

### 3.5 Officially Valid Document as Per PMLA rule 2(d) and 14(i)

"Officially valid document" means the passport, the driving license, the Permanent Account Number (PAN) Card, the Voter's Identity Card issued by Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or **any document as notified by the Central Government in consultation with the regulator**. Where 'simplified measures' are applied for verifying the identity of customers the following documents shall be deemed to be 'officially valid documents':

- (i) identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- (ii) Letter issued by a gazetted officer, with a duly attested photograph of the person;

"No other document will be considered as valid document by the Bank 'simplified measures' may be applied in the case of

'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. In respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any of the documents at (i) and (ii) of proviso to rule 2(d) for the purpose of proof of identity and proof of address."<sup>3</sup>

### 3.6 Transaction:

"Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes-

- (i) Opening of an account;
- (ii) Deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means;
- (iii) The use of a safety deposit box or any other form of safe deposit;
- (iv) Entering into any fiduciary relationship;
- (v) Any payment made or received in whole or in part of any contractual or other legal obligation;
- (vi) any payment made in respect of playing games of chance for cash or kind including such activities associated with casino; and
- (vii) Establishing or creating a legal person or legal arrangement.<sup>14</sup>

### 3.7 Beneficial Owner

- a) Where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

Explanation - For the purpose of this sub-clause-

1. "Controlling ownership interest" means ownership of or entitlement to more than twenty-five percent of shares or capital or profits of the company;

2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;

(b) where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of/entitlement to more than fifteen percent of capital or profits of the partnership;

(c) where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen percent of the property or capital or profits of such association or body of individuals;

(d) Where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

(e) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and

(f) Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.<sup>5</sup>

### 4. Key Elements of the KYC Policy

**KYC Policy** includes the following nine key elements:

1. *Customer Acceptance Policy (CAP)*
2. *Customer Identification Procedures (CIP)*
3. *Monitoring of Transactions*
4. *Risk management*
5. *Training Programme*
6. *Internal Control Systems*
7. *Record Keeping*
8. *Evaluations of KYC guidelines by internal audit and inspection system*
9. *Duties / Responsibilities and Accountability*

### 5. Obligation Under Prevention of Money Laundering (PML) Act 2002

## **5.1 Section 12 of PMLA places certain obligations on Bank, financial institution and intermediary, which include**

- (i) Maintaining a record of prescribed transactions
- (ii) Furnishing information of prescribed transactions to the specified authority
- (iii) Verifying and maintaining records of the identity of its clients
- (iv) Preserving records in respect of (i), (ii) and (iii) above for a period of ten years from the date of cessation of transactions with the clients.

These requirements have come into effect from the 1<sup>st</sup> July, 2005 i.e. the date on which PMLA was notified by the Government of India and rules framed there under.

## **5.2 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) Amendment Rules, 2009–Obligation of Banks/Financial Institutions**

The Government of India vide its Notification No. 13/2009/F.No.6/8/2009- ES dated November 12, 2009, has amended 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.

Some of the salient features of the amendment, relevant to State and Central Co-operative banks/RRBs are as under:

- a) Clause (ca) inserted in sub-rule (1) of Rule 2 defines "non-profit organization"
- b) Clause (BA) inserted in sub-rule (1) of Rule 3 requires banks/ financial institutions to maintain proper record of all transactions involving receipts by non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency.
- c) The amended Rule 6 provides that the records referred to in rule 3 should be maintained for a period of ten years from the date of transactions between the client and the banking company/financial institution.
- d) A provision has been inserted in sub-rule (3) of Rule 8, which requires that banks and its employees should keep the fact of furnishing suspicious transaction information strictly confidential.
- e) Rule 9, now requires banks to verify identity of the non-account based customer while carrying out transaction of an amount equal to or exceeding rupees fifty thousand, whether conducted as a single transaction or several transactions that appear to be connected.
  - i. The amended sub-rule (1) of Rule 9, in terms of clause (b) (ii) requires verification of identity of the customer for **all** international money transfer operations.
  - ii. Proviso to Rule 9(1) regarding the verification of identity of the client within a reasonable time after opening the account/ execution of the transaction **has been deleted.**
- f) "for clause (g), the following clause shall be substituted, namely:-
  - i) "suspicious transactions" means a transaction referred to in clause (h) including an attempted transaction, whether or not made in cash, which to a person acting in good faith.
  - ii) gives rise to a reasonable ground of suspicion that it may involve proceeds of an offence specified in the schedule to the Act, regardless of the value involved; or
- iii) (b) appears to have no economic rationale or bona-fide purpose; or
- iv) (c) Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism."

#### **5.4 Accordingly, in view of amendments to the above Rules, The Jind Central Cooperative Bank Limited Jind will:**

- (i) Maintain proper record of all transactions involving receipts by an entity non-profit organizations of value more than rupees ten lakh or its equivalent in foreign currency and to forward a report to FIU-IND of all such transactions in the prescribed format every month by the 15<sup>th</sup> of the succeeding month.
- (ii) 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. Further, if a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50000/- the bank should verify identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

#### **5.5 Maintaining the Records:**

Bank will maintain records of the identity of clients, and records in respect of transactions with its client referred to in rule 3 in hard or soft format.

#### **5.6 Delay in filing the report**

In terms of Rule 8, while furnishing of information to the Director FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in this rule shall constitute a separate violation.

### **6. Customer Acceptance Policy (CAP)**

Bank's Customer Acceptance policy (**CAP**) lays down the criteria for acceptance of customers. The guidelines in respect of the customer relationship in the Bank are as follows:

- (i) No account is to be opened by Bank in anonymous or fictitious/benami name(s)/entity(ies) { 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 person on whose identity has not been disclosed or cannot be verified.}
- (ii) Bank would not open an account and will close such existing account where 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 the non reliability of the data/ information furnished to the Bank.
- (iii) While carrying out the due diligence it would be ensured that there is no harassment to the customer, only Customer Identification Procedures (discussed later). Necessary checks before opening a new account are to be ensured so that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations available from Circulars, etc.
- (iv) Bank will complete the documentation requirements and will collect other information, as per PMLA and RBI/NABARD guidelines/instructions prevalent .
- (v) Bank would endeavour that Implementation of CAP does not become too restrictive and result in denial of banking services to general public, especially those who are financially or socially disadvantaged and needs to be financially included.



The decision to open an account for Politically Exposed Person (PEP) will be taken at General Manager/ Chief Executive Officer level. Due care will be taken to avoid harassment of the customer and would form a grievances cell for the purpose which will resolve any such issue arising.

For example, decision to close an account may be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

- (vi) Circumstances, in which a customer is permitted to act on behalf of another person/entity, as there can be occasions when an account is operated by a mandate holder or where an account may be opened by an intermediary in the fiduciary capacity has been defined in **Annexure –I (Customer Identification Procedures)**
- (vii) Bank will classify customers into various risk categories based on risk perception, and apply the acceptance criteria for each category of customers. 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 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.
- (viii) Risk perception will be worked out and will be decided for different type of customers taking into account the background of customer/ activity and profile of his/ her clients, country of origin, sources of funds, modes of payments, volume of turnover, social and financial status etc. Of the customer on the basis of the relevant information provided by the customer at the time of opening the account. The intensive due diligence will be required for higher risk customers, especially those for whom the sources of funds are not clear. An indicative risk categories of customers based on customer types is provided in **Annexure-II (Risk category)** which will be reviewed by the Business **Committee of the Bank** on yearly basis.
- (ix) A profile for each customer will be prepared based on risk categorisation. The 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 extend of due diligence would depend on the risk categorisation 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 purpose.
- (x) The indicative information that has to be obtained from customer at the time of opening of account for the purpose of creating customer profile is provided in **Annexure-I (Information for creating customer profile)**. which will be reviewed by the Business **Committee of the Bank** on yearly basis in relevance with the guidelines issued by RBI/ NABARD. The other criterion for the review will be the business requirement and composition of the customers of the Bank.
- (xi) Bank shall accept Customers 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 requirement of PML Act 2002 and instructions/ guidelines issued by RBI/ NABARD/ Bank from time to time.
- (xii) where a customer is categorised as low risk and expresses inability to complete the documentation requirements on account of any reason that the bank considers to be genuine, and where it is essential not to interrupt the normal conduct of business, the bank may complete the verification of identity within a period of six months from the date of establishment of the relationship.

- (xiii) For the purpose of identifying and verifying the identity of customers at the time of commencement of an account-based relationship, Bank may rely on a third party; subject to the conditions that-
- (a) the Bank will immediately obtains necessary information of such client due diligence carried out by the third party;
  - (b) the **Bank** takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the client due diligence requirements will be made available from the third party upon request without delay;
  - (c) the Bank is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with client due diligence and record-keeping requirements in line with the requirements and obligations under the Act;
  - (d) the third party is not based in a country or jurisdiction assessed as high risk; and
  - (e) the Bank is ultimately responsible for client due diligence and undertaking enhanced due diligence measures, as applicable.<sup>9</sup>

## 7. Customer Identification Procedures (CIP)

- 7.1 Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information.
- i) The first requirement of Customer Identification Procedures (**CIP**) is to be satisfied that a prospective customer is actually who he/she claims to be.
  - ii) The second requirement of CIP is to ensure that sufficient information is obtained on the identity and the purpose of the intended nature of the banking relationship.

This would enable risk profiling of the customer and also to determine the expected or predictable pattern of transactions. Satisfactory/ to be satisfied means to be able to satisfy the competent authority that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

- 7.2 Bank will carry out customer identification at different stages viz.
- 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.
- 7.3 Bank will verify the identity for:
- The named account holder
  - Beneficiary account
  - Signatories to account
  - Intermediate parties

- 7.4 Identification data, asunder, would be required to be obtained in respect of different classes of customers:

**7.4.1 For customers that are natural persons:** sufficient identification data would be obtained to verify

- The identity of customer
- His/ her address location
- His/ her recent photographs and
- Documents to verify signature. In case no document is available for verification of the signature, Branch head will obtain signature in his/ her presence.
- Alternatively, identity documents can be substituted by satisfactory personal introduction or where e- KYC has been done except obtaining of photographs.

**7.4.2 For customers that are legal person or entities:**

Sufficient identification data would be obtained to verify:

- Legal status of the legal person/entity through proper and relevant documents.
- That any person purporting to act on behalf of the legal

person/entity is so authorized and identity of that person/entity is established and verified.

- The ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.
- Information on the nature of business activity, location, mode of payments, volume of turn over, social and financial status etc. will be collected for completing the profile of the customer. If the branch/office of The Jind Central Co-operative Bank Ltd. Jind Bank decides to accept such accounts in terms of the Customer Acceptance Policy, the bank would take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manners that it is satisfied that it knows who the beneficial owner(s) is/are.

**7.5** 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.

**7.6** Whenever there shall be any suspicion of money laundering or terrorist financing or where there shall 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 customer/ client and obtaining information on the purpose and intended nature of business relationship.

**7.7** 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.

**7.8** Customer identification data (including photograph/s) shall be periodically updated after the account is opened. The periodicity 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 category customers.

**7.9** Permanent address 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.

## **7.10 Customer identification - Guidelines in respect of few typical cases**

### **7.10.1 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 transaction 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 Clouse (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]. 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 settlers of trust (including any person settling assets into the trust), guarantors 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.

#### **7.10.2 Accounts of companies and firms**

Bank shall be vigilant against business entities being used by individuals as a 'front' for monitoring 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.

#### **7.10.3 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 held. 'Pooled' accounts managed by lawyers/chartered accountants or stock brokers for funds held 'on deposit' or 'in escrow' for arrangement 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".

#### **7.10.4 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. Head of States or Government, senior politicians, senior government/ judicial/ military important political party officials, etc. Sufficient information on any personal 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 should be sought. The decision to open an account for a PEP shall be taken by the concerned Branch 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 Branch 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 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.

#### **7.10.5 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.

#### **7.10.6 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"

#### **7.10.7 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 go in for 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. Money mules' addresses 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 I CFT while opening of accounts and monitoring of transactions to minimize the operations of such mule accounts.

#### 7.10.8 Alternatives / Approvals

No deviations or exemptions shall normally be permitted in the documents specified for account opening. For following 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 extent 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 /RPU (when made operational till such time Branch would continue opening the accounts) after the complete account opening form is received from the branches.

### 8. Monitoring of Transaction

**8.1 Meaning:** Banks are required to report suspicious transactions to the FIU-IND. This requires the Banks to put in place a formal process for identifying suspicious transactions and a procedure for reporting the same internally. This process is known as transaction monitoring.

Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps the banks to know their customers, assess risk and provides greater assurance that the Bank is not being used for the purposes of financial crime. Thus monitoring means analysis of a customer's transactions to detect whether the transactions appear to be suspicious from an AML or CFT.

#### 8.2 Methods of Monitoring:

Bank will adopt following mechanisms to identify suspicious transactions.

- i) Observation: The staff at the bank's branches will at the time of processing the transaction or otherwise come across certain transactions not in line with the profile of the customer. Certain behaviour displayed by the customer during their interactions with such customer may also lead to suspicion. Bank branch staff will report such instances to the principal officers/ his representatives so that additional due diligence may be done on same. A list of behavioural indicators that should trigger suspicion is enclosed as **Annexure IV**.
- ii) AML Software: Bank will have an AML software to generate alerts/ exceptions and then channel these alerts for suitable due diligence and reporting. Alerts concluded to be suspicious might be reported to the FIU-IND through the principal officer.

#### 8.3 Reporting obligation under PMLA

In terms of the Rules notified under Prevention of Money Laundering Act, 2002 (PMLA) certain obligations were cast on banking companies with regard to reporting of certain transactions. The RBI has issued circular No DBOD.NO.AML.BC.63 /14.01.001/2005-06 dated February 15, 2006 and DBOD.AML.BC. No. 85/ 14.01.001 /

2007-08 dated May 22, 2008, detailing the obligation of banks in terms of the Rules notified under PMLA. Accordingly, Banks are required to make the following reports to the FIU-IND.

- \_ Cash Transaction Reporting (CTR)
- \_ Counterfeit Currency Reporting (CCR)
- \_ Suspicious Transaction Reporting (STR)

### 8.3.1 Cash Transaction Reporting (CTR)

As per the PMLA rules, Bank is required to submit the details of:

- a) All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency.
- b) all series of cash transactions integrally connected to each other which have been ***individually<sup>10</sup>*** valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month ***and the monthly aggregate exceeds rupees ten lakh or its equivalent in foreign currency<sup>11</sup>***

The format for reporting of the above-mentioned cash transactions, known as Cash Transaction Report (CTR) has been provided by the RBI vide its circular dated February 15, 2006. This report is required to be filed on a monthly basis by 15th of the succeeding month the Bank will adhere to this.

### 8.3.2 Counterfeit Currency Reporting (CCR)

The PMLA Rule 3(1)(C) read with rule 8 requires the reporting of all cash transactions where forged or counterfeit Indian currency notes have been used as genuine. The RBI vide circular dated May 22, 2008 provided the format in which the CCR needs to be reported to the FIU-IND. The said report is required to be filed not later than ***“had to be reported by the 15<sup>th</sup> day of the succeeding month.”*** from the date of occurrence of such transactions. Bank 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 Bank will adhere to this.

### 8.3.3 Suspicious Transaction Report (STR)

The PMLA Rule 3(1)(D) read with rule 8 requires the reporting of all suspicious transactions whether or not made in cash. Transaction Report (STR) should be furnished within 7 days of arriving at a conclusion that any transaction, is of suspicious nature.

The Principal Officer should record his 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. In determining whether the transaction is suspicious or not, Bank will need the indicators of suspicion. Indicative lists of such indicators are listed in **Annexure V**. In case the STR is repeatedly reported, bank will consider closing the account. However customer should not be tipped off.

### 8.3.4 Cross Border Wire Transfer<sup>13</sup>

All cross border wire transfers of the value of more than rupees five lakhs or its equivalent in foreign currency where either the origin or destination of fund is in India; to be reported to FIU-IND

## 9. Risk Management

The Bank is exposed to reputational, compliance, operational and legal risk if it fails to implement and adhere the KYC and AML standards thus The Jind Central Cooperative Bank Ltd. Will adopt the following guidelines to mitigate these risks

The management of the bank will ensure that appropriate risk-based policies are in place across different aspects of the business. The bank will should adopt an approach to mitigate risk of being used for the purposes of money laundering or terrorist financing. For this it will review the KYC policies from time to time and will take ownership of the risk-based approach, since the management will be held accountable if the approach is inadequate. Business Committee will review the KYC/AML policy from time to time.

9.1 Bank's Internal Audit of compliance with **KYC/AML Policy** will provide an independent evaluation of the same including legal and regulatory requirements.

9.2 The Principal Officer designated by the Bank in this regard will have overall responsibility for maintaining oversight and coordinating with various agencies in this regard.

## 10. Employee Training

Bank would endeavour to train all its employees through internal training and by briefing the employees about the latest updates on the issue of KYC and AML.

10.1 Bank will also facilitate the employees to attend the training programmes conducted by STC/ RICM/ BIRD other such institutes which have the training programmes, having a module on KYC Standards/AML/CFT Measures so that members of the staff are adequately trained in **KYC/AML/CFT** procedures.

10.2 Records will be kept of all formal training conducted. These records will include the names and other relevant details, dates and locations of the training

### 10.3 Recruitment/Hiring of Employees

KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse channels of The Jind Central Co-operative Bank Ltd. Jind. The bank will put in place necessary and adequate screening mechanism as an integral part of its recruitment/hiring process of personnel to ensure that the no such element is recruited or hired who may misuse the channel of the Bank. Bank will have a police verification done for every recruitment/ hiring it makes.

### 10.4 Customer Education

The Jind Central Cooperative Bank Limited Jind recognizes the need to spread awareness on KYC, Anti Money Laundering measures and the rationale behind them amongst the customers and shall take suitable steps for the purpose. The branch staff would be specially trained to educate the customers regarding the objectives of the KYC programme.

## 11. Internal Control and System

11.1 The name, designation and address of the Designated Director will be communicated to the Director, FIU-IND. it shall be the duty of Designated Director, to observe the procedure and manner of furnishing and reporting information on transactions referred to in PML Rule 3.<sup>14</sup>

11.2 Appointment of Principal Officer

The Board of Directors will appoint the GM/ CEO as Principal Officer (PO) who will observe the procedure and manner of furnishing and reporting information on transactions referred to in



- PML Rule 3. The name, designation and address of the Designated Director will be communicated to the Director, FIU-IND <sup>15</sup>
- 11.3 Guidance against "Tipping off"  
Senior management should provide sufficient guidance to staff to ensure that the customers are not informed (i.e. tipped off) that his/her accounts are under monitoring for suspicious activities and/or that a disclosure has been made to the FIU-IND.
- 11.4 Reporting lines will be direct with the (PO) with the minimum number of people between the person with the suspicion and the PO. The speed, confidentiality and accessibility to the PO will be ensured. All procedures will be documented in an appropriate manual or handbook and job descriptions drawn up. All suspicions reported to the PO will be documented (in urgent cases this may follow an initial discussion by telephone). All internal enquiries made in relation to the report, and the reason behind whether or not to submit the report to the FIU-IND, will be documented. This information may be required to supplement the initial report or as evidence of good practice and best endeavors if, at some future date, there is an investigation and the suspicions are confirmed.
- 11.5 What are the roles and responsibilities of the staff  
Staff will be regularly kept abreast with AML information relevant to their role. The communication of a Bank's policies and procedures to its staff to prevent money laundering, and the training in how to apply those procedures, is the key to the success of anti-money laundering strategies.

## 12. Record Keeping

The investigating authorities need to ensure a satisfactory audit trail for suspected money laundering transactions and to be able to establish a financial profile of the suspect account. For example, to satisfy these requirements the following information may be sought by the investigating authorities:

- \_ The beneficial owner of the account;
- \_ The volume of funds flowing through the account;
- \_ For selected transactions:
  - a) The origin of the funds (if known)
  - b) Nature of the transactions;
  - c) The amount of the transactions and the currency in which it was denominated.
  - d) The date on which the transaction was conducted;
  - e) The form in which the funds were offered or withdrawn i.e. cash, cheque etc;
  - f) The identity of the person undertaking the transaction;
  - g) The parties to the transaction;
  - h) The destination of the funds; and
  - i) The form of instruction and authority.

The Jind Central Cooperative Bank Limited Jind will thus maintain the record accordingly and will:

- a) Maintain proper record of all transactions involving receipts by any customer including non- profit organizations of value more than rupees ten lakh or its equivalent in foreign currency and to forward a report to FIU-IND of all such transactions in the prescribed format every month by the 15<sup>th</sup> of the succeeding month.
- b) 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. Further, if a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50000/- the bank should verify identity and

address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

### **13. Evaluations of KYC guidelines by internal audit and inspection system.**

The Internal Audit and Internal Control team of the bank would be responsible to ascertain the effectiveness and efficiency of the AML framework of the bank. This would specifically include checking the adequacy of policies, procedures, and system support to detect suspicious and potential money laundering transactions, and the subsequent monitoring and reporting to regulators, FIU-IND and senior management.

### **14. Duties / Responsibilities and Accountability**

The primary responsibility of ensuring implementation of **KYC/AML/CFT Policy** and related guidelines will be vested with the respective Branch Manager and the Branch staff involved in account opening, however the duties and responsibilities are as given in **Annexure V**.

### **15. Some special cases**

#### **15.1 Small Deposit (No Frills) Accounts:**

With a view to ensuring financial inclusion such that persons, especially those belonging to low income group both in urban and rural areas, who are not able to produce such documents required by the Bank to satisfy about their identity and address, are not denied banking services, branches will open Small Deposit (No Frills) accounts, for natural persons only, with relaxed KYC standards, as detailed in the operating guidelines.

15.1.1 Persons desirous of opening such accounts can keep aggregate balances not exceeding Rs.50000/- (Rupees fifty thousand only) in all their accounts taken together in a financial year.

15.1.2 The aggregate of all withdrawals and transfers in a month does not exceed Rs. 10000/-.

15.1.3 The total credit, again in all accounts taken together, should not exceed Rs. 100000/- (Rupees one lakh only) in a financial year.

If at any point, the above conditions are violated no further transactions will be permitted until full KYC procedure is completed. Bank would notify the customers when the balances reach Rs. 99000/-.

15.1.4 An individual who desires to open a Small account may be allowed to open such account on production of self attested photographs and affixation of signature or thumb print on the account opening form. The Bank would maintain single page account opening application form for the purpose.

15.1.5 The small account will be operational for two years initially and would be reviewed for further extension by the Branch depending upon the requirement by the customer.

### **16. Introduction of New Technologies –**

**Credit cards / debit cards/ smart cards / gift cards.**

16.1 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.

16.2 Bank is engaged in the business of issuing a variety to 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.

### **16.3 Correspondent Banking.**

16.3.1 Correspondent banking is the provision of banking services by on 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, cheque 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.

16.3.2 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 relation ship 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.

16.3.3 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 of 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.

#### **16.3.4 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 shall be applying enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

## **18. Wire Transfer**

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 transfer do not involve actual movement of currency, they are considered as a rapid and secure method for transferring value from one location to another.

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

- a) 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.
- b) 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.
- c) 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.
- d) 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.

18.2 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:

### **18.3 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.

#### **18.4 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.

#### **18.5 Exemptions**

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

#### **18.6 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) 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.

### **19. Combating Financing to Terrorism**

19.1 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.

19.2 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.

## **20. 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, 4<sup>th</sup> 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 email :
- 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 no 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 properly 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 frozen, they shall move an application giving the requisite evidence, in writing to the concerned Bank. The Bank will inform and forward a copy of the application together with full details of assets frozen given by any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, have been frozen inadvertently, to the nodal officer of IS-1 Division of MHA as the contact details given in Paragraph (iv) (b) above within two working days. The Joint Secretary (IS-1), MHA, being the nodal officer for (IS-1) 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.

### **12.1 Jurisdiction that do not or insufficiently apply the FATF Recommendations**

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. I 64771 14.0j .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.

Activity monitoring should cover all accounts including existing accounts for which profiles have not been made.

### **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

@@@@@@@

### Customer identification procedure

Customers 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 along with address proof OR  
Introduction by an existing Bankers (signature Verification report from existing Bank will be required) along with the address proof.
2. **Identity, Signature and Address (ISA) documents 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 to be certified by Branch Head 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 documents wise checks.
3. In order to further ease the difficulties in complying with the KYC requirements, within the overall framework of the Prevention of Money Laundering Act, 2002 (PMLA) and Rules (PMLR), it is clarified as under:
  - (i) Bank will not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorized as 'low risk', in case of no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Bank will not insist on physical presence of such low risk customer at the time of periodic updation.
    - a) In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the RRB/STCB/CCB may take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence / local address. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letter, cheque books,

ATM cards; (ii) telephonic conversation; (iii) visits; etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the RRB/STCB/CCB within two weeks of such a change.

- b) **As regards non-compliance of KYC requirements by the customers:-** If the customer fails to comply KYC requirement despite repeated reminders by bank, bank will impose 'partial freezing' on such KYC non-compliance in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force. While imposing 'partial freezing', bank will ensure that the option of 'partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirement and followed by a reminder for further period of three months. Thereafter, bank will impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts. If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' bank may disallow all debits and credits from/to the accounts, rendering them inoperative. Further, it would always be open to the bank to close the accounts of such customers.<sup>16</sup>

## **RISK CATEGORISATION OF CUSTOMERS**

### **Types of customers and their risk categorisation**

#### **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.
3. Individuals or entities in watch list issued by the Interpol and other similar international organisation.
4. Customers with dubious reputation as per public information available or commercial available watch list.
5. Individuals or entities specifically identify by regulators, FIU and other competent authority ad 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 share (foreign) corporation/business.
12. Non face-to-face customers.
13. High net worth individuals.
14. Partnership Firms.
15. Firms with 'sleeping partner'.
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 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. Account for "gatekeeper" 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 Account managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc.
23. Trusts, charities, NGOs/NPOs (those operating on a "cross border" basis) unregulated clubs and organisation receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies).
24. Money service business: including seller of: Orders/traveller 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 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 cafe, IDD call service, phone card, phone centre.
11. Dot-com company or internet business
12. Pawnshops
13. Auctioneers
14. Cash-intensive Business such as restaurants retails shops, parking garages, fast food stores, movie theatres etc.
15. Sole practitioners or law firms (small, Little known)
16. Notaries (small, Little known)
17. Secretarial (small, Little known)
18. Accountants (small or less 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.

All other categories of accounts/customer not falling under the above indicated High and Medium Risk classifications.

## Customer identification procedure

Customers 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
- iv) Introduction by an existing customer of the Branch having a banking relationship of 6 months or more and having satisfactory conduct of account along with address proof OR
- v) Introduction by an existing Bankers (signature Verification report from existing Bank will be required) along with the address proof.

**1.1 Identity, Signature and Address (ISA) documents 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 to be certified by Branch Head AND any of the officially valid documents which can specify the address and Identity proof.

## LIST OF OFFICIALLY VALID DOCUMENTS

Any one document from the Officially Valid Document is only allowed. They are:

- 1. the passport,
- 2. the driving license,
- 3. the Permanent Account Number (PAN) Card,
- 4. the Voter's Identity Card issued by Election Commission of India,
- 5. job card issued by NREGA duly signed by an officer of the State Government,
- 6. the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number.

It is implied that proof of address also follows from the above documents only.

A proviso has been added to the definition of 'officially valid document' at PML Rule 2(d), which states that where 'simplified measures' are applied for verifying the identity of customers the following documents shall be deemed to be 'officially valid documents':

- i. identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions;
- ii. letter issued by a gazetted officer, with a duly attested photograph of the person;

In terms of Rule 14(i), it has been decided by the Reserve Bank that 'simplified measures' may be applied in the case of

'Low risk' customers taking into consideration the type of customer, business relationship, nature and value of transactions based on the overall money laundering and terrorist financing risks involved. In respect of low risk category of customers, where simplified measures are applied, it would be sufficient to obtain any of the documents at (i) and (ii) of proviso to rule 2(d) for the purpose of proof of identity and proof of address.<sup>17</sup>

Note-<sup>17</sup> list of officially Valid Documents Amended vide BOD Agenda -6 meeting dated 20-1-2017

### Customer identification documents (indicative) –

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.

S.No.	Features	S.No.	Documents
1	Accounts of individuals/HUF- Legal Name or any other name used.	1	Anyone of :-
		i)	Passport (valid)
		ii)	PAN Card
		iii)	Voters identity card
		iv)	Driving License (valid)
		v)	Indian Post ID
		vi)	Government Identity card (subject to the banks satisfaction)
		vii)	Letter from a recognised 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 banks signature verification
		xi)	HUF declaration signed by Karta and Major coparceners including details of minor coparceners along with date of birth.
		xii)	Marriage Certificate / Nikahnama for Women (along with identity documents in Maiden name and valid address proof of the spouse)
		xiii)	Defence Dependents card
		xiv)	Defence Ex-Service Man Card issued to defence 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 bank for more than 6 months with satisfactory conduct of account.

2	Correct Permanent Address	i)	Telephone bill in the name of the customer
		ii)	Bank account statement or passbook
		iii)	Letter from any recognised 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 satisfactory 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:-

S.No.	Features	S.No.	Documents to be taken
3	Minor accounts		Copy of anyone of the following:-
		i)	Birth certificate issued by Municipal authorities
		ii)	Passport
		iii)	PAN card
		iv)	10 <sup>th</sup> or 12 <sup>th</sup> 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 Collage/School/University attesting the identity and signature (letter should have the photograph of students with his signature)
		ix)	Letter from Collage/School/University confirming the address as per their record
4	Non-Resident Indian (NRI) Customers		Copy of:
		i)	Valid Passport & valid Resident/Employment Visa for NRI/NRO Accounts
			<b>In case account opened in person:</b>
		1	Valid Passport with overseas address or work permit (i.e. Green card as residence permit for USA, H1 Visa as work permit for USA or Hong Kong ID card for residence of Hong Kong)
		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.
			<b><u>For persons Employed with Foreign Shipping Companies</u></b>
		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./Airlines\ is prominently displayed.
			<b><u>For Contract Employees</u></b>
		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	Principals overseas address or current work contract.
			<b><u>In case of documents sent by Mail:</u></b>
			All documents/signatures to be attested by any one of the following:
		1	Indian Embassy
		2	Overseas Notary
		3	Local Banker of the NRI
5	Senior Citizens		<b>Copy to:</b>
		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

S.No.	Features	S.No.	Documents to be taken
6	Account of Companies <sup>18</sup>  Note- <sup>18</sup> Cl 6 Amended vide BOD Agenda -6 meeting dated 20-1-2017		a) Certificate of incorporation; b) Memorandum and Articles of Association; c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf; and d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.
	- Name of the company	ii)	Certified true copy of Memorandum of Association and
	- Principal place of business	iii)	Certified true copy of Articles of Association and
	- Mailing address of the company	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 the company Secretary and one director who has attended the said meeting and
	-Telephone/Fax Number	v)	Power of Attorney granted to its managers, officer 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 – from 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 – from 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 & 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 bank for more than 6 months & with satisfactory conduct of account.

S.No.	Features	S.No.	Documents to be taken
7	Accounts of partnership firms - Legal name - Address -Names of all partners and their addresses -Telephone numbers of the firm and partners <sup>19</sup>  Note- <sup>19</sup> Cl 7 Amended vide BOD Agenda -6 meeting dated 20-1-2017	i)	a) Registration certificate; b) Partnership deed; and c) An officially valid document in respect of the person holding an attorney to transact on its behalf.
		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 bank for more than 6 months and with satisfactory of account. HUFs can be partners in current or fixed deposits, however no overdraft to be allowed.

S.No.	Features	S.No.	Documents to be taken
8	Accounts of trusts & foundations -Names of trustees, settlers, beneficiaries, signatories - Names and addresses of the founder, the managers/directors and beneficiaries -telephone/fax number <sup>20</sup> Note- <sup>20</sup> Cl 8 Amended vide BOD Agenda -6 meeting dated 20-1-2017		a) Registration certificate; b) Trust deed; and c) An officially valid document in respect of the person holding a power of attorney to transact on its behalf. e) NOC from the Lending Banker if customer enjoys Credit facilities. f) ISA check of Trustees is not necessary. ISA check is required for all authorized signatories.
9	Accounts of Societies, Clubs & Associations - Names of Authorised Signatories - Names and addresses of the founder, the		a) Resolution of the managing body of such association or body of individuals; b) Power of attorney granted to him to transact on its behalf; c) An officially valid document in respect of the person holding an attorney to transact on its behalf; and

	managers/ directors and the beneficiaries - Telephone / Fax numbers <sup>21</sup>		d) Such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals.
10	Power of Attorney (POA) Holder / Mandate Holder	(i) (ii) (iii) (iv)	Mandate letter signed by the all customers along with the signature of Mandate holder. For POA, duly certified POA agreement along with the signatures of both customer & POA holder. Identity document of the Mandate / POA Holder Photograph of Mandate / POA holder.
11.	Sole Proprietorship Accounts. - Proof of the name of address and activity of the concern.	(i) (ii) (iii) (iv) (v) (vi)  (vii) (i) (ii) (iii) (iv) (v) (vi)  (vii)  (viii) (ix) (x) (xi)  (xii)	Proprietor's complete Identification, Signature and Mailing Address proof documents along with Telephone Number confirmation. Existing current account Bank statement in the same name of the firm) confirming existence of the Firm, Telephone bill confirming address NOC from the Lending Banker if customer enjoys Credit facilities. PAN card with mailing address proof if the initial deposit is in cash. Introduction by Existing Current Account holder who is holding an account with Bank for more than 6 moths and with satisfactory conduct.  <u>Any Two proofs from the below for identity.</u> Registration certificate/licence issued by Municipal authorities such as Shop & Establishment certificate / Trade Licence. CST / VAT / Service Tax Certificate or letter of registration of CST / VAT / Service tax. Certificate/Registration document issued by Service Tax/Professional Tax authorities. Registration certificate (in the case of a registered concern) IEC (Importer Exporter Code) issued by DGFT Certificate / Registration documents issued by Sales Tax / Service Tax / Professional Tax authorities. License issued by the registering authority like certificate of practice issued by Institute of Chartered Accountant of India, Institute of Cost Secretaries of India, India Medical Council, Food and Drug Control Authorities, etc. Licence issued by Explosives Rules. Certificate of registration under any specific Statute / Act of the government. IRDA (Insurance Regulatory and Development Authority) licence in the name of the entity with address mentioned. 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). 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 office 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 Centre 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 acknowledge.
		(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

		(xxix)	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.
		(xxx)	Registration Certificate / Licence issued by Rubber Board / Spices Board / Tea Board / Coffee Board / Coir Board / Tobacco Board / National Jute Board / Pollution Control Board. 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
12. Government Accounts	<p>A.) Accounts of Executive Engineers / SDO (Assistant Engineer) / BDPO (Block Development &amp; Panchayat Officers / DDPO (Distt. Development &amp; Panchayat Officer):</p> <ol style="list-style-type: none"> <li>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 &amp; disbursal officer), And.</li> <li>2. Letter of Intent signed by Executive Engineer / SEO / BDPO / DDPO to open an account with Bank or the immediate officer (reporting authority) would issue a letter confirming that an official is authorized to open and operate the account, And</li> <li>3. Letter of Intent signed by Executive Engineer / SDO / BDPO / DDPO to open an account with bank.</li> </ol> <p>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.</p> <ol style="list-style-type: none"> <li>1. Letter of Intent signed by SDM / DC to open an account with Bank, And</li> <li>2. Government order / circular confirming the name and designation of SDM / DC.</li> </ol> <p><u>C) Account in the name of Estate Officer:</u> If SDM and DC hold charge of the Estate Officer, then</p> <ol style="list-style-type: none"> <li>1. Letter of Intent signed by SDM / DC to open an account with Bank, And</li> <li>2. Letter confirming that the Deputy ?Commissioner works as the Estate Officer, And</li> <li>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....”</li> </ol> <p>Additionally (not mandatory)</p> <ol style="list-style-type: none"> <li>1. ISA of authorized signatories.</li> <li>2. Self-signed Cheque.</li> </ol> <p>All accounts need to be signed by Branch Head confirming that they have met the concerned officials.</p>

### Customer Behaviour Indicators

- \_ Customers who are reluctant in providing normal information while opening an account, providing minimal or fictitious information or when applying to open an account, providing information that is difficult or expensive for the institution to verify.
- \_ Customer expressing unusual curiosity about a secrecy of information involved in the transaction.
- \_ Customers who decline to provide information that in normal circumstances would make the customer eligible for banking services.
- \_ Customer giving confusing details about a transaction.
- \_ Customer reluctant or refuses to state a purpose of a particular large / complex transaction/ source of funds involved or provides a questionable purpose and / or source.
- \_ Customers who use separate tellers to conduct cash transaction or foreign exchange transactions.
- \_ Customers who deposit cash / withdrawals by means of numerous deposit slips / cheques leaves so that the total of each deposits is unremarkable, but the total of all credits / debits is significant.
- \_ Customer's representatives avoiding contact with the branch.
- \_ Customers who repay the problem loans unexpectedly.
- \_ Customers who appear to have accounts with several institutions within the same locality without any apparent logical reason.
- \_ Customers seeks to change or cancel a transaction after the customer is informed of currency transaction reporting / information verification or record keeping requirements relevant to the transaction.
- \_ Customer regularly issues large value cheques without balance and then deposits cash.

The above list is illustrative and not exhaustive. The Principal Officer of the Branch/Office of The Jind Central Co-operative Bank Ltd. Jind where suspicious activity/transaction is reported should verify their port depending upon the circumstances of the activity/transaction reported and satisfy himself whether the activity/ transaction is to be reported as a suspicious activity/transaction or is to be treated as a bonafide one. Care should be taken that the customers with bonafide transactions are not inconvenienced.

## **An Indicative List of Suspicious Activities**

### **Transactions Involving Large Amounts of Cash**

- (i) Exchanging an unusually large amount of small denomination notes for those of higher denomination;
- (ii) Purchasing or selling of foreign currencies in substantial amounts by cash settlement despite the customer having an account with the bank;
- (iii) Frequent withdrawal of large amounts by means of cheques, including traveller's cheques;
- (iv) Frequent withdrawal of large cash amounts that do not appear to be justified by the customer's business activity;
- (v) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad;
- (vi) Company transactions, both deposits and withdrawals, that are denominated by unusually large amounts of cash, rather than by way of debits and credits normally associated with the normal commercial operations of the company, e.g. cheques, letters of credit, bills of exchange etc.;
- (vii) Depositing cash by means of numerous credit slips by a customer such that the amount of each deposit is not substantial, but the total of which is substantial.

### **Transactions that do not make Economic Sense**

- (i) A customer having a large number of accounts with the same bank, with frequent transfers between different accounts;
- (ii) Transactions in which assets are withdrawn immediately after being deposited, unless the customer's business activities furnish a plausible reason for immediate withdrawal.

### **Activities not consistent with the Customer's Business**

- (i) Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
- (ii) Corporate accounts where deposits & withdrawals by cheque/telegraphic transfers/foreign inward remittances/any other means are received from/ made to sources apparently unconnected with the corporate business activity/dealings.
- (iii) Unusual applications for DD/TT/PO against cash.
- (iv) Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.
- (v) Retail deposit of many cheques but rare withdrawals for daily operations.

### **Attempts to avoid Reporting/Record-keeping Requirements**

- (i) A customer who is reluctant to provide information needed for a mandatory report, to have the report filed or to proceed with a transaction after being informed that the report must be filed.
- (ii) Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.
- (iii) An account where there are several cash deposits/withdrawals below a specified threshold level to avoid filing of reports that may be necessary in case of transactions above the threshold level, as the customer intentionally splits the transaction into smaller amounts for the purpose of avoiding the threshold limit.



## **Unusual Activities**

- (i) An account of a customer who does not reside/have office near the branch even though there are bank branches near his residence/office.
- (ii) A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
- (iii) Funds coming from the list of countries/centres, which are known for money laundering.

## **Customer who provides Insufficient or Suspicious Information**

- (i) A customer/company who is reluctant to provide complete information regarding the purpose of the business, prior banking relationships, officers or directors, or its locations.
- (ii) A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
- (iii) A customer who has no record of past or present employment but makes frequent large transactions.

## **Certain Suspicious Funds Transfer Activities**

- (i) Sending or receiving frequent or large volumes of remittances to/from countries outside India.
- (ii) Receiving large TT/DD remittances from various centres and remitting the consolidated amount to a different account/centre on the same day leaving minimum balance in the account.
- (iii) Maintaining multiple accounts, transferring money among the accounts and using one account as a master account for wire/funds transfer.

## **Certain Bank Employees arousing Suspicion**

- (i) An employee whose lavish lifestyle cannot be supported by his or her salary.
- (ii) Negligence of employees/willful blindness is reported repeatedly. Some examples of suspicious activities/transactions to be monitored by the operating staff-

\_ Large Cash Transactions

\_ Multiple accounts under the same name

\_ Frequently converting large amounts of currency from small to large denomination notes

\_ Placing funds in term Deposits and using them as security for more loans

\_ Large deposits immediately followed by wire transfers

\_ Sudden surge in activity level

\_ Same funds being moved repeatedly among several accounts

\_ Multiple deposits of money orders, Banker's cheques, drafts of third parties

\_ Multiple deposits of Banker's cheques, demand drafts, cross/ bearer cheques of third parties into the account followed by immediate cash withdrawals

\_ Transactions inconsistent with the purpose of the account

\_ Maintaining a low or overdrawn balance with high activity

Check list for preventing money-laundering activities:

\_ A customer maintains multiple accounts, transfer money among the accounts and uses one account as a master account from which wire/ funds transfer originates or into which wire/funds transfer are received (a customer deposits funds in several accounts, usually in amounts below a specified threshold and the funds are then consolidated into one master account and wired outside the country).

\_ A customer regularly depositing or withdrawing large amounts by a wire transfer to, from, or through countries that are known sources of narcotics or where Bank secrecy laws facilitate laundering money.

\_ A customer sends and receives wire transfers (from financial haven countries) particularly if there is no apparent business reason for such transfers and is not consistent with the customer's business or history.

\_ A customer receiving many small incoming wire transfer of funds or deposits of cheques and money orders, then orders large outgoing wire transfers to another city or country.

\_ A customer experiences increased wire activity when previously there has been no regular wire activity.

\_ Loan proceeds unexpectedly are wired or mailed to an offshore Bank or third party.

\_ A business customer uses or evidences or sudden increase in wire transfer to send and receive large amounts of money, internationally and/or domestically and such transfers are not consistent with the customer's history.

\_ Deposits of currency or monetary instruments into the account of a domestic trade or business, which in turn are quickly wire transferred abroad or moved among other accounts for no particular business purpose.

\_ Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.

\_ Instructing the Bank to transfer funds abroad and to expect an equal incoming wire transfer from other sources.

\_ Wiring cash or proceeds of a cash deposit to another country without changing the form of the currency

\_ Receiving wire transfers and immediately purchasing monetary instruments prepared for payment to a third party.

\_ Periodic wire transfers from a person's account/s to Bank haven countries.

\_ A customer pays for a large (international or domestic) wire transfers using multiple monetary instruments drawn on several financial institutions.

\_ A customer or a non-customer receives incoming or makes outgoing wire transfers involving currency amounts just below a specified threshold, or that involve numerous Bank or travellers cheques

\_ A customer or a non customer receives incoming wire transfers from the Bank to 'Pay upon proper identification' or to convert the funds to bankers' cheques and mail them to the customer or non-customer, when

\_ The amount is very large (say over Rs.10 lakhs)

\_ The amount is just under a specified threshold (to be decided by the Bank based on local regulations, if any)

\_ The funds come from a foreign country or

\_ Such transactions occur repeatedly.

A customer or a non-customer arranges large wire transfers out of the country which are paid for by multiple Bankers' cheques (just under a specified threshold)

A Non-customer sends numerous wire transfers using currency amounts just below a specified threshold limit.

The above list is illustrative and not exhaustive. The Principal Officer of the Branch/Office of The Jind Central Co-operative Bank Ltd. Jind where suspicious activity/transaction is reported should verify the report depending upon the circumstances of the activity/transaction reported and satisfy himself whether the activity/ transaction is to be reported as a suspicious activity/transaction or is to be treated as a bonafide one. Care should be taken that the customers with bonafide transactions are not inconvenienced.

**DUTIES/RESPONSIBILITIES AND ACCOUNTABILITY****The importance of KYC guidelines to the employees**

The **Bank** employees will conduct themselves in accordance with the highest ethical standards and in accordance with the extant regulatory requirements and laws. Staff and management shall not provide advice or other assistance to individuals who are indulging in money laundering activities. The chain of duties and responsibilities at branches/controlling offices and accountability are as under and non-compliance of the duties and responsibilities arising out of KYC guidelines will lead to fixation of accountability. Dereliction of duty and avoidance of knowledge will lead to examination of staff accountability.

**Personnel****Duties/Responsibilities**

Officer in Charge of accounts/

To interview the potential customer

Officer vested with the

To verify the introductory authority to open new accounts customer profile reference/

To arrive at threshold limits for each account (new as well as existing) and to exercise due diligence in identifying suspicious transactions.

To ensure against opening of accounts in the names of terrorist/banned organizations

To adhere to the provisions of Foreign Contribution Regulatory Act 1976.

To comply with the guidelines issued by the bank from time to time in **respect** of opening and conduct of account.

Branch Manager

To scrutinize and satisfy himself/ herself the information furnished in the account opening form/customer profile/threshold limit are in strict compliance with KYC guidelines before authorizing opening of account.

To certify in the Statement/Register regarding compliance with KYC guidelines and report suspicious transactions to appropriate authority.

Concurrent Auditor

To verify and record his comments on the effectiveness of measures taken by branches/level of implementation of KYC guidelines

Controlling Authority

Prompt reporting of information regarding suspicious transactions to the law enforcing authority concerned in consultation with Principal Officer at Head Office.

Name of Financial Institution:

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

Information submitted to:

<b>I</b>	<b>General Information</b>	
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 F1 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 on electronic address, a post office address or an accommodation address) and in a country in which bank employees one or more individuals fill 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 F1 have a legal and regulatory compliance program that includes a designation compliance officer who is responsible for coordinating and overseeing the AML programme, on a day-to-day basis, which has been approved by Senior Management of the F1?		
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 F1? IF YES, ESTABLISHED DATE: REVIEWED DATE:		
6	In addition to inspections by the government supervisors/regulators, does the F1 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		

**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) was 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) 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;*
- (b) 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",*

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), Ministry of Home Affairs. His contact details are 011-23092736 (Tel), 011-23092569 (Fax) and jsis@nic.in (e-mail id).
- (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.
- (iv) 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.
- (v) 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.
- (vi) 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.
- (vii) 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 IS-I 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 FIUIND.

**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, herein after, 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 id: [jsis@nic.in](mailto:jsis@nic.in)
- (iii) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall also send 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 FIU-IND, 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 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 id: [jsis@nic.in](mailto:jsis@nic.in).
- (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 are 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 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 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 would necessarily be conveyed on e-mail id: [jsis@nic.in](mailto:jsis@nic.in).

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 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 id: [jsis@nic.in](mailto:jsis@nic.in). 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 there quisite 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 15 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 the 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 .Dipti vilasa)  
Joint Secretary to Government of India

1. Governor Reserve Bank of India. Mumbai
2. Chairman Security Exchange Board of India, Mumbai.
3. Chairman Insurance Regulatory Authority, Hyderabad.
4. Foreign Secretary, Ministry of External Affairs, New Delhi.
5. Finance Secretary, Ministry of Finance, New Delhi.
6. Revenue Secretary, Department of Revenue, Ministry of Finance, New Delhi.
7. Director Intelligence Bureau, New Delhi.
8. Additional Secretary, Department of Financial Services, Ministry of Finance, New Delhi.
9. Chief Secretary of All States/Union Territory.

All Non Banking Financial Companies /  
Residuary Non Banking Companies

Dear Sir,

**Implementation of Section 51-A of UAPA, 1967- Splitting of UNSC 1267 Committee's list of individuals and entities linked to Al-Qaida and Taliban**

Please refer to the UN Security Council's 1267 Committee's Consolidated List of individuals and entities linked to Al-Qaida and Taliban who are subject to the assets freeze, travel ban and arms embargo as set out in relevant Security Council Resolution 1822 (2008). Pursuant to being included in the 1267 Committee's Consolidated List these individuals and entities are subject of action under Section 51A of the Unlawful Activities (Prevention) Act, 1967.

2. The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in **splitting of the Consolidated List into two separate lists**, namely:

(i) **"Al-Qaida Sanctions List"**, which is maintained by the 1267 / 1989 Committee. This List shall include only the names of those individuals, groups, undertakings and entities associated with Al-Qaida. General information on the work of the committee is available at <http://www.un.org/sc/committees/1267/information.shtml>. The Updated Al-Qaida Sanctions List is available at [http://www.un.org/sc/committees/1267/aq\\_sanctions\\_list.shtml](http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml)

(ii) **"1988 Sanctions List"**, which is maintained by the 1988 Committee. This list consists of names previously included in Sections A ("Individuals associated with the Taliban") and B("Entities and other groups and undertakings associated with the Taliban") of the Consolidated List. The Updated 1988 Sanctions list is available at <http://www.un.org/sc/committees/1988/list.shtml>

3. It may be noted that both "Al-Qaida Sanctions List" and "1988 Sanctions List" are to be taken into account for the purpose of implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967.

4. This information is being issued in pursuance of the instructions contained in the Ministry of Home Affairs (Internal Security-I Division), Government of India's order F. No. 17015/10/2002-IS-IV, dated 27 August 2009, regarding the Procedure for implementation of Section 51A of the Unlawful Activities(Prevention) Act, 1967.

5. NBFCs are required to update the lists of individuals/entities as circulated by Reserve Bank and before opening any new account, it should be ensured that the name/s of the proposed customer does not appear in either list. Further, NBFCs should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the two lists.

Yours faithfully,

(Dr Tuli Roy)  
Deputy General Manager

October 21, 2014

The Chairperson / Chief Executive Officers  
All Scheduled Commercial Banks (Excluding RRBs)/ Local Area Banks /  
All India Financial Institutions

Dear Madam/Sir

**Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT) guidelines – clarifications on periodic updation of low risk customers, non-requirement of repeated KYC for the same customer to open new accounts and partial freezing of KYC non-compliant accounts**

Reserve Bank has been simplifying the KYC norms from time to time, in order to ease the difficulties faced by common persons while opening bank accounts and complying with periodic updation requirements. It has, however, been brought to the notice of the Reserve Bank that despite such measures and various attempts by banks in this direction, customers are still facing difficulties in complying with the periodic updation requirements. Further, it is also reported that there are still many KYC non-compliant accounts due to non-submission of KYC documents by customers at the time of periodical updation. This often leads to KYC non-compliant accounts continuing to be operated and making them vulnerable to money-laundering and terrorist financing activities.

2. In this context, a reference is invited to paragraphs 31 and 32 ([extracts enclosed](#)) of the Fourth Bi-Monthly Monetary Policy Statement, 2014-15, announced on September 30, 2014, on easing norms to be followed during periodic updation and introduction of 'partial freezing' on KYC non-compliant accounts.

3. In terms of our [circular DBOD.AML.BC.No.39/14.01.001/2013-14 dated September 4, 2014](#) on 'Client Due Diligence', the requirement of applying client due diligence measures to existing clients at an interval of two/eight/ten years in respect of high/medium/low risk clients respectively, would continue taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained. In order to further ease the difficulties in complying with the KYC requirements, within the overall framework of the Prevention of Money Laundering Act, 2002 (PMLA) and Rules (PMLR), it is clarified as under:

(i) Banks need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorised as 'low risk', in case of no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Banks may not insist on physical presence of such low risk customer at the time of periodic updation.

(ii) If an existing KYC compliant customer of a bank desires to open another account in the same bank, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose.

4. As regards non-compliance of KYC requirements by the customers despite repeated reminders by banks, it has been decided that banks should impose 'partial freezing' on such KYC non-compliant in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force. While imposing 'partial freezing', banks are advised to ensure that the option of 'partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirement and followed by a reminder for further period of three months. Thereafter, banks may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts. If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' banks may disallow all debits and credits from/to the accounts, rendering them inoperative. Further, it would always be open to the bank to close the account of such customers.

5. Banks may revise their KYC policy in the light of the above instructions and ensure strict adherence to the same.

Yours faithfully

(Lily Vadera)  
Chief General Manager

October 31, 2014

Regional Rural Banks (RRBs) /  
State / Central Cooperative Banks (StCBs/CCBs)

Madam / Dear Sir,

**Know Your Customer (KYC) Norms /Anti-Money Laundering (AML) Standards/ Combating of Financing of Terrorism (CFT) guidelines – clarifications on periodic updation of low risk customers, non-requirement of repeated KYC for the same customer to open new accounts and partial freezing of KYC non-compliant accounts**

Reserve Bank has been simplifying the KYC norms from time to time, in order to ease the difficulties faced by common persons while opening bank accounts and complying with periodic updation requirements. It has, however, been brought to the notice of the Reserve Bank that despite such measures and various attempts by banks in this direction, customers are still facing difficulties in complying with the periodic updation requirements. Further, it is also reported that there are still many KYC non-compliant accounts due to non-submission of KYC documents by customers at the time of periodical updation. This often leads to KYC non-compliant accounts continuing to be operated and making them vulnerable to money-laundering and terrorist financing activities.

2. In this context, a reference is invited to paragraphs 31 and 32 ([extracts enclosed](#)) of the Fourth Bi-Monthly Monetary Policy Statement, 2014-15, announced on September 30, 2014, on easing norms to be followed during periodic updation and introduction of 'partial freezing' on KYC non-compliant accounts.

3. In terms of our [circular RPCD.RRB.RCB.AML.BC.No.31/07.51.018/2014-15 dated September 9, 2014](#) on 'Client Due Diligence', the requirement of applying client due diligence measures to existing clients at an interval of two/eight/ten years in respect of high/medium/low risk clients respectively, would continue taking into account whether and when client due diligence measures have previously been undertaken and the adequacy of data obtained. In order to further ease the difficulties in complying with the KYC requirements, within the overall framework of the Prevention of Money Laundering Act, 2002 (PMLA) and Rules (PMLR), it is clarified as under:

- i. RRBs and StCBs/CCBs need not seek fresh proofs of identity and address at the time of periodic updation, from those customers who are categorized as 'low risk', in case of no change in status with respect to their identities and addresses. A self-certification by the customer to that effect should suffice in such cases. In case of change of address of such 'low risk' customers, they could merely forward a certified copy of the document (proof of address) by mail/post, etc. Banks may not insist on physical presence of such low risk customer at the time of periodic updation.
- ii. If an existing KYC compliant customer of a bank desires to open another account in the same bank, there should be no need for submission of fresh proof of identity and/or proof of address for the purpose.
- iii. 4. As regards non-compliance of KYC requirements by the customers despite repeated reminders by banks, it has been decided that banks should impose 'partial freezing' on such KYC non-compliance in a phased manner. Meanwhile, the account holders can revive accounts by submitting the KYC documents as per instructions in force. While imposing 'partial freezing', banks are advised to ensure that the option of 'partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirement and followed by a reminder for further period of three months. Thereafter, banks may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts. If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' banks may disallow all debits and credits from/to the accounts, rendering them inoperative. Further, it would always be open to the bank to close the accounts of such customers.

5. RRBs and StCBs/CCBs may revise their KYC policy in the light of the above instructions and ensure strict adherence to the same.

Yours faithfully,

(Madhavi Sharma)  
Chief General Manager

Encl. as above

