Policy on

Know Your Customer Norms

&

Anti-Money Laundering Standards

J&K Bank

Serving To Empower

For complete details visit **www.jkbank.com** or call toll free **1800 1800 234**

Follow J&K Bank on:

Table of Contents

Annexures

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
EDD	Enhanced Due Diligence
CTR	Cash Transaction Report
NTR	Non-Profit Organization Transaction Report
NGO	Non-Governmental Organization
CCR	Counterfeit Currency Report
MLRO	Money Laundering Reporting Officer
PO	Principal Officer
CBWT	Cross Border Wire transfer
OVD	Officially valid Document

1.0 Context

1.1 Money laundering has acquired a global character that not only threatens security, but also compromises the stability, transparency and efficiency of financial systems. Across the world, banks and financial institution are required to introduce and implement system to prevent anti-social elements from using banking channels for money laundering. In India, consolidated anti-money laundering specific legislation, Prevention of Money laundering Act, 2002 (PMLA) came into effect with the Government of India Gazette notification on 1st of July 2005. The Financial Intelligence Unit-India (FIU-IND) constituted by Government of India on 18th of November 2004 as a nodal agency for anti-money laundering measure also got statutory recognition on 1st of July 2005.

1.2 Bank has updated policy in place on "Know Your Customer-Anti Money Laundering Standards" reflecting the regulatory changes made till 09th August 2019 approved by the Board in October 2019. The policy is based on the revised guidelines issued by Reserve Bank of India in the amendments to Master Direction (MD) on Know Your Customer (KYC), 2016 dated 29th May 2019 and 9th August 2019 and is subject to annual review.

2.0 Purpose

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

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

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

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

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

3.0 Scope of the Policy

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

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

3.3 Details of Designated Director and Principal Officer of the Bank as required under the Prevention of Money Laundering (PML) Act 2002 read with Rules 2005 have been published on the banks Intranet under Featured Items option "Director & Principal Officer for PML". The same is available at below web link:

http://reports.jkb.com/jkbcms/executeLink?linkId=4768 (Press Ctrl +Click to open the link)

3.4 This policy should be read in conjunction with internal circulars issued by the Bank on the subject from time to time.

4.0 Definitions

4.1. Money Laundering

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

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

4.2. Transaction

Transaction as per Rule 2(h) of PML act 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;

vii) Establishing or creating a legal person or legal arrangement.'

4.3. Person

In terms of PML Act a 'person' includes:

(i) an individual,

(ii) a Hindu undivided family,

(iii) a company,

(iv) a firm,

(v) an association of persons or a body of individuals, whether incorporated or not,

(vi) every artificial juridical person, not falling within any one of the above persons (i to v), and

(vii) any agency, office or Business Unit owned or controlled by any of the above persons (i to vi).

4.4. Customer

For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with Bank and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

4.5. Suspicious Transaction

"Suspicious transaction" means a "transaction" including an attempted transaction, whether or not made in cash which to a person acting in good faith;

- gives rise to reasonable ground of suspicion that it may involve proceeds of crime, regardless of the value involved; or

- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to have no economic rationale or bonafide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism which includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

4.6. Officially valid document (OVD)

As per RBI's revised guidelines, documents spelt out as "Officially Valid Documents" shall only be accepted for opening of new account. No discretion to accept any other document for the account opening purpose shall be exercised by the Business Unit official/s. It is implied that proof of address also follows from the "Officially Valid Document" only.

"Officially Valid Document" (OVD) means:

1. The passport
2. The driving licence
3. Proof of possession of Aadhaar number.
4. The Voter's Identity Card issued by the Election Commission of India
5. Job card issued by NREGA duly signed by an officer of the State Government and
6. Letter issued by the National Population Register containing details of name and address.

Provided that,

a. Where the customer submits his proof of possession of Aadhaar number as an OVD, he may submit it in such form as are issued by the Unique Identification Authority of India.
b. where the OVD furnished by the customer does not have updated address, the following documents shall be deemed to be OVDs for the limited purpose of proof of address:-
   i. utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
   ii. property or Municipal tax receipt;
   iii. pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
   iv. letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies and leave and licence agreements with such employers allotting official accommodation;
c. the customer shall submit OVD with current address within a period of three months of submitting the documents specified at 'b' above
d. where the OVD presented by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

   Explanation: For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

(i) Provided that where 'simplified measures' are applied for verifying the identity of the clients the following documents shall be deemed to be OVD:

   a. 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;

   b. Letter issued by a Gazetted officer, with a duly attested photograph of the person.

(ii) Provided further that where 'simplified measures' are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be OVD :

a. Utility bill which is not more than two months old of any service provider (electricity, telephone, post-paid mobile phone, piped gas, water bill);
b. Property or Municipal Tax receipt;

c. Bank account or Post Office savings bank account statement;
d. Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address;
e. Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and
f. Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India.

4.7. Certified Copy of OVD

Obtaining a certified copy by the Business Unit shall mean comparing the copy of officially valid document (OVD) so produced by the customer with the original and recording the same on the copy by the authorised officer of the bank.

Provided that in case of Non-Resident Indians (NRIs) and Persons of Indian Origin (PIOs), as defined in Foreign Exchange Management (Deposit) Regulations, 2016 {FEMA 5(R)}, alternatively, the original certified copy of OVD, certified by any one of the following, may be obtained:

- authorised officials of overseas branches of Scheduled Commercial Banks registered in India,
- branches of overseas banks with whom Indian banks have relationships,
- Notary Public abroad,
- Court Magistrate,
- Judge,
- Indian Embassy/Consulate General in the country where the non-resident customer resides.

4.8. Customer Due Diligence (CDD)

Customer Due Diligence (CDD) means identifying and verifying the customer and the beneficial owner.

4.9. Aadhaar number

"Aadhaar number", as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means an identification number issued to an individual under sub-section (3) of section 3 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), and includes any alternative virtual identity generated under sub-section (4) of that section.

Further, "Authentication", means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

4.10. Offline Verification

"Offline Verification", as defined in the Aadhaar and Other Law (Amendment) Ordinance, 2019, means the process of verifying the identity of the Aadhaar number through such offline modes as specified by the Aadhaar regulations.

4.11. Beneficial Owner (BO)

a. Where the customer is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical persons, has/have a controlling ownership interest or who exercise control through other means.

Explanation- For the purpose of this sub-clause-

1. "Controlling ownership interest" means ownership of/entitlement to more than 25 per cent of the

shares or capital or profits of the company.

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

b. Where the customer 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/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.

c. Where the customer 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/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

Explanation: Term 'body of individuals' includes societies. Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.

d. Where the customer is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

For detailed information regarding identification & incorporation of Beneficial Owner details in CBS refer to Annexure-VI of this policy.

4.12 Other Definitions

Terms bearing meaning assigned in this Directions, unless the context otherwise requires, shall bear the meanings assigned to them below:

i) "Walk-in Customer" means a person who does not have an account-based relationship with the Bank, but undertakes transactions with the Bank.

ii) "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.

iii) "Customer identification" means undertaking the process of CDD.

iv) "FATCA" means Foreign Account Tax Compliance Act of the United States of America (USA) which, inter alia, requires foreign financial institutions to report about financial accounts held by U.S. taxpayers or foreign entities in which U.S. taxpayers hold a substantial ownership interest.

v) "IGA" means Inter Governmental Agreement between the Governments of India and the USA to improve international tax compliance and to implement FATCA of the USA.

vi) "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the Central KYC Registry (an entity defined to receive, store, safeguard and retrieve the KYC records in digital form of a customer), for individuals and legal entities.

vii) "Non-face-to-face customers" means customers who open accounts without visiting the branch / offices of the Bank or meeting the officials of the Bank.

viii) "On-going Due Diligence" means regular monitoring of transactions in accounts to ensure that they are consistent with the customers' profile and source of funds.

ix) "Periodic Updation" means steps taken to ensure that documents, data or information collected under the CDD process is kept up-to-date and relevant by undertaking reviews of existing records at periodicity prescribed by the Reserve Bank.

x) "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States / Governments, senior politicians, senior government / judicial / military officers, senior executives of state-owned corporations, important

political party officials, etc.

xi) "Regulated Entities" (REs) means

xii) all Scheduled Commercial Banks (SCBs) / Regional Rural Banks (RRBs) / Local Area Banks (LABs) / All Primary (Urban) Co-operative Banks (UCBs) / State and Central Co-operative Banks (StCBs / CCBs) and any other entity which has been licenced under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks'

xiii) All India Financial Institutions (AIFIs)

xiv) All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs).

xv) All Payment System Providers (PSPs) / System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers)

xvi) All authorised persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

xvii) "Shell bank" means a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group.

xviii) "Wire transfer" means a transaction carried out, directly or through a chain of transfers, 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.

xix) "Domestic and cross-border wire transfer": When the originator bank and the beneficiary bank is the same person or different person located in the same country, such a transaction is a domestic wire transfer, and if the 'originator bank' or 'beneficiary bank' is located in different countries such a transaction is cross-border wire transfer.

Note:

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Banking Regulation Act, 1949, the Reserve Bank of India Act, 1935, the Prevention of Money Laundering Act, 2002, the Prevention of Money Laundering (Maintenance of Records) Rules, 2005, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and regulations made thereunder and 'Aadhaar and other Laws (amendment) Ordinance, 2019', any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

5.0 KYC Policy Guidelines

5.1 General

i. Confidentiality of customer information: Bank shall keep in view that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Bank shall, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer shall be sought separately with his / her consent and after opening the account. 'Mandatory' information required for KYC purpose which the customer is obliged to give while opening an account only should be obtained at the time of opening the account/during periodic updation. Other 'optional' customer details/additional information, if required may be obtained separately after the account is opened only with the explicit consent of the customer. The customer has a right to know what is the information required for KYC that she/he is obliged to give, and what is the additional information sought by the bank that is optional.

ii. Avoiding hardship to customers: While issuing operational instructions to Business Units, bank will keep in mind the spirit of the instructions issued by the Reserve Bank so as to avoid undue hardships to individuals who are otherwise classified as low risk customers.

iii. Sensitizing customers: Implementation of AML/CFT policy may require certain information from customers of a personal nature or which had not been called for earlier. The purpose of collecting such information could be questioned by the customer and may often lead to avoidable complaints and litigation. Business Unit to prepare specific literature/pamphlets, etc., to educate the customer regarding the objectives of the AML/CFT requirements for which their cooperation is solicited

iv. Bank shall ensure that any remittance of funds by way of demand draft, mail / telegraphic transfer or any other mode and issue of travelers' cheques /sale of gold coins, etc. for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment.

v. Bank shall not make payment of cheques/drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.

vi. Bank shall ensure that the provisions of Foreign Contribution (Regulation), as amended from time to time, wherever applicable are strictly adhered to.

5.2 Key Elements of KYC Policy:

The KYC Policy includes the following four key elements

i. Customer Acceptance Policy (CAP)

ii. Customer Identification Procedures (CIP)

iii. Monitoring of Transactions; and

iv. Risk Management

5.3 Customer Acceptance Policy (CAP)

The following Customer Acceptance Policy indicating the criteria for acceptance of customers shall be followed in the bank. The Business Units shall accept customers strictly in accordance with the said policy.

i) No account shall be opened in anonymous or fictitious/benami name(s). (i.e. the persons whose identity has not been disclosed or cannot be verified)

ii) Parameters of risk perception are clearly defined by the Bank for appropriate risk categorization. For the purpose of Risk Categorization, the basic requirements of verifying the identity and location of the customers, sources of income, transactions in the accounts, etc shall be considered, as detailed in Para 5.4 of this policy.

iii) Documentation requirements and other information to be collected in respect of different categories of customers are detailed in Annexure-I.

iv) The Business Units will not open an account or close an existing account where the bank is unable to apply appropriate customer due diligence (CDD) measures i.e. bank is unable to verify the identity, verifying the customer and the beneficial ownership and / or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data / information furnished to the bank.

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

vi) Business Units should also consider closing existing accounts under similar situations. Decision for closure of such accounts shall be taken at Zonal Office level after giving due notice to the customer explaining the reasons for such a decision by the concerned business unit.

vii) CDD Procedure shall be followed by the Business Units for all the joint account holders, while opening a joint account.

viii) Circumstances in which a customer is permitted to act on behalf of another person/entity shall be clearly spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an account is opened by an intermediary in fiduciary capacity.

Under following circumstances / occasions, a customer shall be permitted to act on behalf of another person / entity, an account shall be permitted to be operated by a mandate holder or permitted to be opened by an intermediary in fiduciary capacity;

a) Accounts operated by power of attorney holders on the strength of duly registered POA wherein identity of the POA holder is verified by the bank.

b) Accounts operated as per mandate of the account holder, who has tendered the mandate before the bank officials and wherein identity of the mandate holder is verified by the bank.

ix) Business Units shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organizations & the sanctioned individuals/ entities etc. RBI has been circulating lists of terrorist entities notified by the Government of India so that banks exercise caution against any transaction detected with such entities. The Business Units shall invariably consult such lists to ensure that prospective person/s or organizations desirous to establish relationship with the bank are not in any way involved in any unlawful activity and that they do not appear in such lists. The updated UN consolidated list shall be kept available on the Bank's Intranet page under the head "Documents & Manuals" for that purpose. The existing accounts shall be periodically scanned against the latest available UN Consolidated lists using AMLOCK software by KYC/ AML Department and in case of any positive matches; procedure laid down in UAPA order dated March 14, 2019 (Annexure-V) shall be strictly followed.

x) The mandatory information for KYC purpose while opening an account and during the periodic updation, shall be obtained by the Business Units. 'Optional' / additional information, shall be obtained with the explicit consent of the customer after the account is opened. The Business Units shall prepare a profile for each new customer based on risk categorization. The bank has devised a revised Composite Account Opening Form for recording and maintaining the profile of each new customer. Revised form is separate for Individuals, Partnership Firms, Joint Accounts, Corporates and other legal entities or special accounts e.g., account in the name of brand names, domain names, etc. The customer profile may contain information relating to customer's identity, social / financial status, nature of business

activity, information about his clients business and their location etc. The nature and extent of due diligence shall depend on the risk perceived by the business unit. However, while preparing customer profile business units shall take care to seek only such information from the customer, which is relevant to the risk category and beneficial ownership and is not intrusive. The Business Units should continue to follow strictly the instructions issued by the bank regarding secrecy of customer information.

xi) In case of KYC compliant customers there shall be no need for a fresh Customer Due Diligence (CDD) for opening more than one account under single Customer Id (CUST ID).

Note:

Implementation of Customer Acceptance Policy should not become too restrictive and must not result in denial of banking services to the general public, especially to those, who are financially or socially disadvantaged.

5.4 Risk Perception in respect of Customer

"Customer risk" in the present context refers to the money laundering and terrorist funding risk associated with a particular customer from a Bank's perspective. This risk is based on risk perceptions associated with customer profile and the level of risk associated with the product & channels used by Customer. For categorizing a customer as low risk, medium risk and high risk, the parameters considered are location of customer and his client, mode of payments, nature of activity, volume of turnover and social and financial status.

I. Low Risk Customers (Level 1 customers)

Individuals (other than High Net worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large confirm to the known profile may be categorized as Low risk such as:

- Salaried employees
- People belonging to lower economic strata of the society
- Government Departments
- Government owned companies
- Regulatory and Statutory bodies, etc.

II. Medium Risk Customers (Level 2 customers):

Customers who are likely to pose a higher than average risk to the bank should be categorized as medium or high risk. For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his/her client profile, beneficial ownership etc. besides proper identification.

The following customers are classified as Medium Risk Customers:

- Gas Dealers
- Car/boat/plane dealers
- Electronics
- Travel agency
- Telemarketers
- Telecommunication service providers
- Pawnshops
- Auctioneers

- Restaurants, Retail shops, Movie theatres, etc.
- Sole practitioners
- Notaries
- Accountants
- Blind
- Purdanashin

III. High Risk Customers (Level 3 customers):

For this category, higher due diligence is required which includes customer's background, nature and location of activity, country of origin, source of funds and his client profile, beneficial ownership etc. besides proper identification. Bank shall subject such accounts to enhanced monitoring on an ongoing basis. The following customers are classified as High Risk Customers:

- Trusts, charities, NGOs and organizations receiving donations.
- Companies having close family shareholding or beneficial ownership
- Firms with 'sleeping partners'.
- Accounts under Foreign Contribution Regulation Act.
- Politically Exposed Persons (PEPs).
- Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
- Those with dubious reputation as per public information available.
- Accounts of non-face-to-face customers, etc.
- High Net worth Individuals*
- Non-Resident customers.
- Accounts of Cash intensive businesses such as accounts of bullion dealers (Including sub-dealers) & jewelers.

* Parameters for defining High Net worth Individuals:

Customers with any of the following:

I) Average balance of Rs. 2.00 lakh and above in SB/NRE SB.

II) Balance of Rs. 10.00 lakh and above in Term deposit, Domestic/NR.

III) Balance of Rs.5.00 lakh and above in CA.

IV) Enjoying Fund based limits/term loans exceeding Rs. 30.00 lakh.

V) Salary credit of Rs. 1, 00,000/- and above in a Super saving salary A/c.

VI) Business contribution/opinion makers /VIPs such as head of

Village/Town/City, Top Executives of Companies etc.

The categorization of customers under risk perception is only illustrative and not exhaustive. The Business Units may categorize the customers according to the risk perceived by them while taking into account the above aspects. For instance, a salary class individual who is generally to be classified under low risk category may be classified otherwise based on the perception of the Business Unit/Office. RBI has directed that Banks are required to prepare a Risk profile of each customer and apply enhanced due diligence measures on High risk customers. IBA has provided an indicative list of High/Medium risk Products, Services, Geographies, locations, etc., for Risk Based Transaction Monitoring by Banks (detailed in Annexure-III & IV).

IV. Customer Risk Categorization

Bank may select the parameters based on the available data. Once the parameters are finalized, Bank may choose the appropriate risk rating/scoring models by giving due weightage to each parameter. Bank shall adopt combination of manual and automatic classification. Based on the availability of data, Bank shall finalize parameters which are available in the system and the same shall be reviewed annually. AML System shall assign provisional risk categorization based on the CBS system provided parameters. Business Units shall review the same and make suitable modification/revision, if need be, based on remaining indicators as covered in the policy.

Risk categorization shall be under taken by the business units based on parameters such as customer's identity, Social/Financial status, nature of business activity, information about the clients' business and their location etc. While considering customer's identity, the ability to confirm identity documents through online or other services offered by issuing authorities may also be factored in.

The nature and extent of due diligence will depend on the risk perceived by the Bank. Risk categorization shall be done based on selection of parameters and assigning suitable risk category.

Risk Parameters

The first step in process of risk categorization is selection of parameters, which would determine customer risk.

IBA Core Group on KYC and AML in its guidance note for Banks on KYC/AML/CFT obligation of Banks under PMLA 2002 has suggested following indicative parameters which can be used to determine the profile and risk category of Customers:

1. Customer Constitution: Individual, Proprietorship, Partnership, Private Ltd.

etc.

2. Business Segment : Retail, Corporate etc

3. Country of residence/Nationality: Whether India or any overseas location/Indian or foreign national.

4. Product Subscription: Salary account, NRI products etc.

5. Economic Profile: HNI, Public Ltd. Company etc.

6. Account Status: Active, inoperative.

7. Account Vintage: Less than six months old etc.

8. Presence in regulatory negative/PEP/Defaulters/Fraudster lists.

9. Suspicious Transaction Report (STR) filed for the customer.

10. AML alerts.

Other parameters like source of funds, occupation, purpose of account opening, nature of business, mode of operation, credit rating etc can also be used in addition of the above parameters. Bank shall adopt all or majority of these Parameters based on availability of data.

Risk rating of Customers

Bank shall ensure to classify Customers as Low Risk, Medium Risk and High Risk depending on background, nature and location of activity, country of origin, Sources of funds and client profile etc.

A. An Illustrative list of Low/Medium/High Risk Customers, Products, Services, Geographies, etc., based on the recommendations of IBA Working Group on Risk Based Transaction Monitoring is detailed in Annexure IV.

B. Risk rating based on the Deposits/account balance:

As per IBA Working Group guidelines, Banks may choose to carry out either manual classification or automatic classification or a combination of both. Similarly for selecting parameters,

Account Types	*High*	*Medium*	*Low*
Only SB*	Rs.2,00,000/- & above	Rs. 1,00,000/- & above but less than Rs.2,00,000/-	Less than Rs.1,00,000/-
Only Current*	Rs.5,00,000/- & above	Rs. 2,00,000/- & above but less than Rs.5,00,000/-	Less than Rs.2,00,000/-
Only Term Deposits	Rs.10,00,000/ & above	Rs. 5,00,000/- & above but less than Rs.10,00,000/-	Less than Rs.5,00,000/-

*Applicable in case of accounts having completed 6 months

For Current/SB accounts average balance for last 6 months and for Term Deposits principal amount shall be taken for consideration on the date of review. If a customer is having more than one of the above categories of accounts, highest risk assigned as per the above parameter shall be the overall risk for this parameter. For ex: A customer having a savings account with average balance of Rs.1,50,000/-(medium) and Term Deposit of Rs.4,00,000/-(low) shall have rating of Medium Risk for this parameter.

Above categorization of the Customer shall be based on all accounts linked to CUST ID irrespective of constitution of account like Joint account, Partnership account etc. However accounts linked to CUST ID where customers do not have any stake in Business/activity need not be clubbed for the above purpose.

C. Risk Categorization of the customers shall be done according to the risk perceived while taking into account the above aspects. For instance, a salaried class individual who is generally to be classified under low risk category may be classified otherwise based on following illustrative list of parameters considered as "High Risk" such as:

- Unusual transaction/behavior (given as Annexure-II – Monitoring of Customer Risk Categorization (CRC).
- Submitted Suspicious Transaction Reports (STR) for Customer.
- Submitted Cash Transaction Report (CTR).
- Frequent Cheque returns.
- Minor.

D. Risk Categorization of customers shall be based on combination of above parameters, i.e., mentioned under A, B & C above. Among the chosen parameters, highest risk grade will be assigned as overall Risk for the customer. For ex: a Travel Agent (Medium risk) with Proprietorship account (low risk) and having Savings account with average balance of Rs.1,50,000/-(medium risk) and Term Deposit of Rs.4,00,000/- (low risk) , shall be assigned with overall rating of "Medium Risk", provided all other conditions mentioned under C above does not necessitate for assigning "High Risk".

Risk categorization of Customers undertaken by the Bank:

Based on the policy/guidance notes of RBI/IBA (as detailed under points A, B & C above), risk rating shall be assigned taking into account the following parameters available in CBS system :

- Customer type.
- Customer Constitution.
- Occupation.
- Product code.
- Account status
- Account vintage.
- Average balance/deposits in SB/Current/Term Deposit accounts.

V. Roles and responsibilities of Business Units:

Monitoring/Review of Customer Risk Categorization (CRC):

Business Units shall carry out a review of risk categorization of customers at aperiodicity of not less than once in six months. Such review for the first half of the financial year i.e. April to September shall be undertaken in succeeding November, and for the second half the financial year i.e. October to March in succeeding May in every financial year. During such review, the risk assigned to an existing customer may undergo change depending on the change in risk parameters of the customer. Wherever there is suspicion at Business Unit level that a prospective Customer is above low risk, Business Units should carry out customer due diligence (CDD) before opening an account. Based on objective parameters for enhanced due diligence, Business Units shall arrive at a conclusion whether the transaction is suspicious or not. Some of the objective parameters for enhanced due diligence could be:

- Customer locations.
- Financial Status.

- Nature of business.
- Purpose of transaction.
- Beneficial ownership

The IBA Working Group had recommended alert indicators for detection of suspicious transactions for implementation by all the Banks. However 27 alert indicators pertain to off-line transactions and Business Units shall submit the STR's out of 27 offline alert scenarios in the prescribed STR format. The list of 27 offline alert indicators is provided in Annexure-II and Monitoring of Customer Risk Categorization (CRC) – given as Annexure-III.

5.5 Threshold Limit

Threshold limit, as the name indicates, means an upper limit of single transaction which is normally expected from a customer. The limit shall be fixed on the basis of interaction/profile when the relationship is established with the prospective customer. For example, for a person drawing monthly salary of Rs. 50,000/- a threshold limit of Rs. 50,000/- can be fixed; for a businessman, habitual of carrying transactions between Rs. 5.00 Lacs to 10.00 Lacs, a threshold limit of Rs. 10.00 Lacs can be fixed; for a high net worth customer, a threshold limit of Rs. 1.00 Crore or above can be fixed. The limit so fixed shall appropriately be mentioned in Composite Account Opening Form. The limits discussed above are indicative and while fixing threshold limits, the operative levels shall be solely guided by the perception they conceive while perusing the profile of the customer and interaction they have with the prospective customer. Once transaction crosses the Threshold Limit, enquiry shall be conducted and reasons thereof shall be recorded or if deemed fit Suspicious Transaction Report shall be raised. The threshold limit shall be revised as per requirement.

6.0 Customer Identification Procedure (CIP)

General

(a) Customer Identification Procedure means:

Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial ownership on the basis of one of the OVDs. Bank to obtain sufficient information to establish, to its satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of the banking relationship and be satisfied that due diligence has been observed based on the risk profile of the customer in compliance with the extant guidelines in place. Such risk based approach is to avoid disproportionate cost to bank and a burdensome regime for the customers. Besides obtaining of valid proof of address, an independent verification of address will also to be carried out, by sending "Welcome Kit" to the customer.

(b) Customer Identification Procedure to be carried out at different stages

- While establishing a banking relationship (or)
- Carrying out a financial transaction (or)
- When there is a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data.
- When bank sells third party products as agent;
- While selling bank's own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for more than Rs. 50,000/-.
- When carrying out transactions for a non-account based customer, that is a walk-in customer, where the amount involved is equal to or exceeds Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected.
- When the bank has a reason to believe that a customer (account- based or walk-in) is intentionally structuring a transaction into a series of transactions below the threshold of Rs. 50,000/-.
- Carrying out any international money transfer operations for a person who is not an account holder of the bank.

- Identity to be verified for:
  - (a) The named account holder
  - (b) Beneficiary account
  - (c) Signatories to an account
  - (d) Intermediate parties

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

- the identity of the customer,
- his / her address/location
- his / her recent photograph

For customers that are legal persons or entities -

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

Further, Records or the information of the customer due diligence carried out by the third party is obtained within two days from the third party or from the Central KYC Records Registry.

6.1 Customer Due Diligence (CDD) Procedure

6.1.1 Customer Due Diligence (CDD) Procedure for Individuals

For undertaking CDD, Business Units shall obtain the following from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorised signatory or the power of attorney holder related to any legal entity :

(a) a certified copy of OVD containing details of his identity and address
(b) Two recent photographs for Account Opening Form & Passbook.
(c) the Permanent Account Number (PAN) or Form No. 60 (as defined in Income-tax Rules, 1962), and
(d) such other documents pertaining to the nature of business or financial status as specified by the Bank in Annexure –I to this policy.

Provided that,

i) Business Units shall obtain the Aadhaar number from an individual who is desirous of receiving any benefit or subsidy under any notified Government scheme. Business Units, at receipt of the Aadhaar number from the customer may carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India upon receipt of the customer's declaration that he is desirous of receiving any benefit or subsidy under any scheme notified under section 7 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies Benefits and Services) Act, 2016 (18 of 2016) in his account.
ii) Business Units may carry out Aadhaar authentication / offline-verification of an individual who voluntarily uses his Aadhaar number for identification purpose. However, Business Units shall ensure that the customers (non-DBT beneficiaries) while submitting Aadhaar as OVD, redact or blackout their Aadhaar number in terms of sub-rule 16 of Rule 9 of the amended PML Rules.

A. OTP Based e-KYC for in non-face-to-face Customers

Accounts opened using OTP based e-KYC, in non face to face mode are subject to the following conditions:

(i) There must be a specific consent from the customer for authentication through OTP.
(ii) the aggregate balance of all the deposit accounts of the customer shall not exceed rupees one lakh. In case, the balance exceeds the threshold, the account shall cease to be operational, till CDD as mentioned at (v) below is complete.
(iii) the aggregate of all credits in a financial year, in all the deposit taken together, shall not exceed rupees two lakh.
(iv) As regards borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned shall not exceed rupees sixty thousand in a year.
(v) Accounts, both deposit and borrowal, opened using OTP based e- KYC shall not be allowed for more than one year within which identification as per the proper CDD measures stated above at Section 5.1.1 is to be carried out.
(vi) If the CDD procedure as mentioned above is not completed within a year, in respect of deposit accounts, the same shall be closed immediately. In respect of borrowal accounts no

further debits shall be allowed.

(vii) A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC in non-face-to-face mode with any other Regulated Entity. Further, while uploading KYC information to CKYCR, The operating officials of the Bank shall clearly indicate that such accounts are opened using OTP based e-KYC and other Banks shall not open accounts based on the KYC information of accounts opened with OTP based e-KYC procedure in non-face-to-face mode.

B. Small Accounts

In case an individual customer who does not possess any of the OVDs and desires to open a bank account, banks shall open a 'Small Account'. A 'Small Account' means a savings account which entails the following limitations:

i) the aggregate of all credits in a financial year does not exceed rupees one lakh;
ii) the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand; and
iii) the balance at any point of time does not exceed rupees fifty thousand.
iv) Provided, that this limit on balance for Small Accounts shall not be considered while making deposits through Government grants, welfare benefits and payment against Government procurements.

Further, small accounts are subject to the following conditions:

(a) The Business unit shall obtain a self-attested photograph from the customer.
(b) The concerned officer of the bank shall certify under his signature that the person opening the account has affixed his signature or thumb impression in his presence. The Master Directions on KYC updated on 09-08-2019 read with Government Notification G.S.R 381(E) dated 28-05-2019 regarding amendment to PML (Maintenance of Records) Rules 2005 provides that where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature and the account shall remain operational on annual submission of certificate of proof of address issued by the officer in-charge of the jail.
(c) Such accounts are opened only at Core Banking Solution (CBS) linked branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to the account.
(d) The bank shall ensure that the stipulated monthly and annual limits on aggregate of transactions and balance requirements in such accounts are not breached, before a transaction is allowed to take place.
(e) The account shall remain operational initially for a period of twelve months which can be extended for a further period of twelve months, provided the account holder applies and furnishes evidence of having applied for any of the OVDs during the first twelve months of the opening of the said account.
(f) The entire relaxation provisions shall be reviewed after twenty four months.
(g) The account shall be monitored and when there is suspicion of money laundering or financing of terrorism activities or other high risk scenarios, the identity of the customer shall be established through the production of an OVD and Permanent Account Number or Form No.60, as the case may be.
(h) Foreign remittance shall not be allowed to be credited into the account unless the identity of the customer is fully established through the production of an OVD and Permanent Account Number or Form No.60, as the case may be.

6.1.2 Customer Due Diligence (CDD) Procedure for Sole Proprietary firms

For opening an account in the name of a sole proprietary firm, CDD of the individual (proprietor) shall be carried out.
In addition to the above, any two of the following documents as a proof of business/ activity in the name of the proprietary firm shall also be obtained:

i) Registration certificate
ii) Certificate/licence issued by the municipal authorities under Shop and Establishment Act.
iii) Sales and income tax returns.
iv) CST / VAT / GST certificate (provisional/final).

v) Certificate/registration document issued by Sales Tax / Service Tax / Professional Tax authorities.
vi) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT / Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute.
vii) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities.
viii) Utility bills such as electricity, water, and landline telephone bills.

In cases where the Business Units are satisfied that it is not possible to furnish two such documents, Business Unit may, at their discretion, accept only one of those documents as proof of business/activity. Provided Business Units undertake contact point verification and collect such other information and clarification as would be required to establish the existence of such firm, and shall confirm and satisfy itself that the business activity has been verified from the address of the proprietary concern.

6.1.3 Customer Due Diligence (CDD) Procedure for Legal Entities

A. Customer Due Diligence (CDD) Procedure for Company Accounts

For opening an account of a company, certified copies of each of the following documents shall be obtained:

(a) Certificate of incorporation
(b) Memorandum and Articles of Association
(c) Copy of Permanent Account Number (PAN) in the name of the company duly validated in PAN/TAN application of the bank.
(d) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf.
(e) Documents of the managers, officers or employees holding an attorney to transact on the company's behalf are required as per CDD procedure for individuals (defined under section 6.1.1 of this policy).

Business Units to remain vigilant against business entities being used by individuals as a 'front' for maintaining accounts with bank. Business Unit to examine 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. These requirements are to be moderated according to the risk perception e.g. in the case of a public company it is not necessary to identify all the shareholders.

B. Customer Due Diligence (CDD) Procedure for Partnership firms

For opening an account of a partnership firm, the certified copies of each of the following documents shall be obtained:

(a) Registration certificate
(b) Partnership deed
(c) Copy of Permanent Account Number (PAN) in the name of the partnership firm duly validated in PAN/TAN application of the bank.
(d) Documents of the person holding an attorney to transact on the behalf of the firm are required as per CDD procedure for individuals (defined under section 6.1.1 of this policy).

C. Customer Due Diligence (CDD) Procedure for Trusts

For opening an account of a trust, certified copies of each of the following documents shall be obtained:

(a) Registration certificate
(b) Trust deed
(c) Copy of Permanent Account Number (PAN) in the name of the Trust duly validated in PAN/TAN application of the bank or Form No.60.
(d) Documents of the person holding an attorney to transact on the behalf of the firm are required as per CDD procedure for individuals (defined under section 6.1.1 of this policy).

Further in cases of trust/nominee or fiduciary accounts whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary is determined. In such cases satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also details of the nature

of the trust or other arrangements in place shall be obtained.

D. Customer Due Diligence (CDD) Procedure for unincorporated association or a body of individuals

For opening an account of an unincorporated association or a body of individuals, certified copies of each of the following documents shall be obtained:

(a) Resolution of the managing body of such association or body of individuals
(b) Copy of Permanent Account Number (PAN) in the name of the unincorporated association or a body of individuals duly validated in PAN/TAN application of the bank or Form No.60.
(c) Power of attorney granted to transact on its behalf
(d) Documents of the person holding an attorney to transact on its behalf are required as per CDD procedure for individuals (defined under section 6.1.1 of this policy) and
(e) Such information as may be required by the Business Unit to collectively establish the legal existence of such an association or body of individuals from documents like memorandum of Association/ Deed/byelaws or any other document of said nature.

Explanation: Unregistered trusts / partnership firms shall be included under the term 'unincorporated association'.

Explanation: Term 'body of individuals' includes societies.

E. Customer Due Diligence (CDD) Procedure for Juridical Persons not covered above

For opening accounts of juridical persons not specifically covered in the earlier part, such as societies, universities and local bodies like village panchayats, certified copies of the following documents shall be obtained:

(a) Document showing name of the person authorised to act on behalf of the entity;
(b) Documents of the person holding an attorney to transact on its behalf are required as per CDD procedure for individuals (defined under section 6.1.1 of this policy) and
(c) Such documents as may be required by the Bank to establish the legal existence of such an entity / juridical person.

A gist of documents that can be accepted as proof of identity and address for various categories is furnished in Annexure I.

F. Other Measures

(i) For opening accounts of individuals, Business units to obtain one certified copy of an 'officially valid document' containing details of identity and address, one recent photograph and such other documents pertaining to the nature of business and financial status of the customer as may be required.

(ii) E-KYC service of Unique Identification Authority of India (UIDAI) is also accepted as a valid process for KYC verification under the PML Rules. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process is treated as an 'Officially Valid Document'. Under e-KYC, the UIDAI transfers the data of the individual comprising name, age, gender, and photograph of the individual, electronically to the bank/business correspondents/ business facilitators, which is accepted as valid process for KYC verification.

(iii) Since introduction is not necessary for opening of accounts under PML Act and Rules or the

Reserve Bank's extant instructions, Business units will not insist on introduction for opening of bank accounts. However, the due diligence at the time of accepting a customer is of utmost importance to avoid frauds. Spirit of KYC norms is to ensure the authenticity of OVD for identity and address of the customer. A certificate of having verified genuineness of OVD must be appended on the photocopy of the documents and kept with AOF.

(iv) A customer is required to submit only one OVD for both proof of identity and for proof of address as part of KYC procedure. If the OVD submitted for proof of identity does not have the proof of address (for e.g., PAN Card), then the customer is required to submit another OVD for proof of address.

(v) Similarly, A customer shall not be required to furnish separate proof of current address, if it is different from the address recorded in the OVD. In such cases, the business unit shall merely obtain a declaration from the customer indicating the address to which all correspondence will be made by the bank. However, as per customer verification process, the business units must verify the current address through the acknowledgment of receipt of 'Welcome Kit" sent to the recorded current address of the customer as per declaration.
In case the address mentioned as per 'proof of address' undergoes a change, fresh proof of address is to be submitted to the Business units within a period of six months. Business Units shall display a notice prominently in their Business Unit Premises to intimate customers that in the event of change in address due to relocation or any other reason, they should intimate the new address to the bank within two weeks of such a change. While opening new accounts and while periodically updating KYC data as required in terms of the KYC/AML/CFT guidelines, an undertaking to this effect should be obtained.

(vi) Business units will not insist to obtain fresh documents of the customer when the customer approaches it for transferring his/her account from one Business Unit to another Business Unit. Business units will ensure that KYC verification once done by the transferor Business Unit will be valid for the transferee Business Unit if full KYC verification has been done for the concerned account and is not due for periodic updation. Further, if an existing KYC compliant customer desires to open another account in the bank, there is no need for fresh CDD exercise.

(vii) Accounts of Politically Exposed Persons (PEPs) resident outside India:

a) Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public positions/functions in a foreign country, e.g., Heads of States or of Governments, Senior politicians, Senior Government/Judicial/Military officers, Senior Executives of state-owned corporations, important political party officials etc. Business units will ensure enhanced due diligence and will gather sufficient information on any person/customer of the category of PEPs intending to establish a banking relationship and try to collect and check all information available on the person in the public domain. Business units will also verify the identity of the person and seek information about the sources of funds before accepting PEP as customer. Such accounts will be subjected to enhanced monitoring on an ongoing basis.

b) In the event of existing customers or the beneficial owner of an existing account subsequently becoming a PEP, the approval of the Executive manager and above will be obtained to continue the business relationship and subject the account to the enhanced due diligence measures as applicable to the customers of PEP category including enhanced monitoring on an on-going basis. The said norms will also apply to the accounts of the family members or close relatives of PEPs. Such type of Customers requiring very high level of monitoring will be categorized as 'High Risk'. These instructions are also applicable to accounts where PEP is the ultimate beneficial owner.

(viii) Accounts of Non-face-to-face customers:

In case of non-face-to-face customers, in addition to the usual customer identification procedures, enhanced due diligence shall be ensured. Bank shall ensure that the first payment is to be effected through the customer's KYC-complied account, for enhanced due diligence of non-face to face customers.

In the case of cross-border customers, the Bank will ensure that the third party certifying the

supporting documents is regulated and supervised entity and has adequate KYC systems in place.

(ix) 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 twenty thousand, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. If there is a reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.20,000/-, identity and address of the customer shall be verified and filing a suspicious transaction report (STR) to FIU-IND may be considered. The identity and address of the Walk-in customer is to be verified by obtaining KYC documents and records are to be maintained/ updated in the system.

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

(x) Verification of OVD's

a. Business Unit should verify the genuineness of "Officially Valid Document/s" (including PAN Card) submitted by customer while opening of accounts or updating its profile. Self-attested Copies of the submitted OVD's must be verified with the originals and officials accepting such documents should invariably put a stamp "Verified with the original(s)" under his/her signature with date. PAN of the customer must be authenticated on the income tax web portal enabled through bank's intranet. Confirmatory web page so obtained must be kept on record with CRF.

b. Welcome Kit
In respect of all newly opened accounts, a "Welcome Kit" shall be sent to the new account holder through registered AD and the acknowledgment received thereof must be placed on record with the CRF. This would while earning the goodwill of the customer also serve as a verification/confirmation of address.
If the Welcome Kit so sent is returned undelivered, the debit operations in such accounts must be stopped and the reason thereof shall be intimated to the customer through a phone call or any other mode of communication.

6.1.4. Enhanced and Simplified Due Diligence Procedure

Enhanced Due Diligence

A. Accounts of non-face-to-face customers:

Business Units/Bank shall ensure that the first payment is to be effected through the customer's KYC-complied account with another Bank, for enhanced due diligence of non-face-to-face customers.

B. Accounts of Politically Exposed Persons (PEPs)

Business Units shall have the option of establishing a relationship with PEPs provided that:

(a) sufficient information including information about the sources of funds accounts of family members and close relatives is gathered on the PEP;
(b) the identity of the person shall have to be verified before accepting the PEP as a customer;
(c) the decision to open an account for a PEP is taken at a senior level in accordance with the Bank's Customer Acceptance Policy;
(d) all such accounts are subjected to enhanced monitoring on an on-going basis;
(e) In the event of an existing customer or the beneficial owner of an existing account subsequently becoming a PEP, the approval of the Executive manager and above shall be obtained to continue the business relationship and the enhanced due diligence measures

as applicable to the customers of PEP category including enhanced monitoring on an on-going basis;

(f) the CDD measures as applicable to PEPs including enhanced monitoring on an on-going basis are applicable. The said norms will also apply to the accounts of the family members or close relatives of PEPs. Such type of Customers requiring very high level of monitoring will be categorized as 'High Risk'.

These instructions shall also be applicable to accounts where a PEP is the beneficial owner.

C. Pooled Accounts- Client accounts opened by professional intermediaries:

Business Units shall ensure while opening client accounts through professional intermediaries, that:

(a) Clients shall be identified by applying the KYC norms when client account is opened by a professional intermediary on behalf of a single client.
(b) Business Units shall have option to hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds.
(c) Business Units shall not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the Bank.
(d) All the beneficial owners shall be identified where funds held by the intermediaries are not co-mingled at the level of Bank, and there are 'subaccounts', each of them attributable to a beneficial owner, or where such funds are co-mingled at the level of Bank, the Business units shall look for the beneficial owners.
(e) The ultimate responsibility for knowing the customer lies with the bank.

Simplified Due Diligence

D. Simplified norms for Self Help Groups (SHGs)

a) CDD of all the members of SHG shall not be required while opening the savings bank account of the SHG.
b) CDD of all the office bearers shall suffice.

No separate CDD of the members or office bearers shall be necessary at the time of credit linking of SHGs.

E. Procedure to be followed for opening accounts of foreign students

Business units will follow the following procedure for foreign students studying in India:

(1) Business units will open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India.
(2) Business units will obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address.
(3) During the 30 days period, the account will be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.
(4) The account shall be treated as a normal NRO account, and shall be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of FEMA 1999 (The Foreign Exchange Management Act, 1999 (42 of 1999)).
(5) Students with Pakistani nationality will need prior approval of the Reserve Bank for opening the account.

F. Simplified KYC norms for Foreign Portfolio Investors (FPIs)

Accounts of FPIs which are eligible / registered as per SEBI guidelines, for the purpose of investment under Portfolio Investment Scheme (PIS), shall be opened by accepting KYC documents as detailed in Annexure I (A), subject to Income Tax (FATCA / CRS) Rules.

Provided that the Business Unit shall obtain undertaking from FPIs or the Global Custodian acting on behalf of the FPI that as and when required, the exempted documents as detailed in Annexure I (A) will be submitted.

6.1.5. Beneficial Ownership

When the Bank identifies a customer for opening an account, it will identify the beneficial owner(s) and take all reasonable steps in terms of Rule 9(3) of the PML Rules to verify his identity, as per guidelines provided below:

(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/have 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/entitlement to more than 25 per cent of the shares or capital or profits of the company
2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements.

(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/have ownership of/entitlement to more than 15 per cent 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/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.

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

(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 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

(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.

There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, bank will determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, bank will insist on satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. The different categories of beneficiaries should be identified as defined above. In the case of a 'foundation', steps should be taken to verify the founder managers/ directors and the beneficiaries, if defined.

For detailed information regarding identification & incorporation of Beneficial Owner details in CBS refer to Annexure-VI of this Policy.

6.2 Introduction of New Technology Products -

(Internet Banking / Credit Cards / Debit Cards / Smart Cards / Gift Cards)

a) Bank will pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking. The Bank will not provide internet facility/technology product to any person without compliance of KYC guidelines and without customer's specific request/understanding of the product. Bank will ensure that full KYC/AML procedures are duly applied before providing internet facility / issuing credit cards / debit cards / smart cards / gift cards etc. including on the add-on/supplementary cardholders.

b) The amount transferred / received through electronic mode, beyond a threshold limit, of Rs 50,000/- (fifty thousand rupees) and above would be to the debit of the accounts of the customers concerned.

6.3 Periodical Updation of customer Profile:

(A) CDD Requirements for Periodic Updation

Periodic updation shall be carried out at least once in every two years for high risk customers, once in every eight years for medium risk customers and once in every ten years for low risk customers as per the following procedure:

S.No	Risk Level	Due for Periodic Updation
1.	**High Risk**	**2 Years**
2.	**Medium Risk**	**8 Years**
3.	**Low Risk**	**10 Years**

(a) Business Units shall carry out

i. PAN verification from the PAN/TAN verification facility available in the CBS, and

ii. Authentication, of Aadhaar Number already available with the Bank with the explicit consent of the customer in applicable cases.

iii. In case identification information available with Aadhaar does not contain current address an OVD containing current address may be obtained.

iv. Certified copy of OVD containing identity and address shall be obtained at the time of periodic updation from individuals not eligible to obtain Aadhaar, except from individuals who are categorized as 'low risk'. In case of low risk customers when there is no change in status with respect to their identities and addresses, a self-certification to that effect shall be obtained.

(b) In case of Legal entities, Business Unit shall review the documents sought at the time of opening of account and obtain fresh certified copies.

Business Units may not insist on the physical presence of the customer for the purpose of furnishing OVD or furnishing consent for Aadhaar authentication unless there are sufficient reasons that physical presence of the account holder/holders is required to establish their bona-fides. Normally, OVD/Consent forwarded by the customer through mail/post, etc., shall be acceptable.

(c) Business Units shall ensure to provide acknowledgment with date of having performed

KYC updation.

(d) The time limits prescribed above would apply from the date of opening of the account/ last verification of KYC.

6.4 Miscellaneous

(i) At par cheque facility availed by co-operative banks.

Business Units having arrangements with co-operative banks wherein the latter open current accounts with the bank and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for effecting their remittances and payments. Since the 'at par' cheque facility offered by bank to co-operative banks is in the nature of correspondent banking arrangement, Business units will monitor and review such arrangements to assess the risk including credit risk and reputational risk arising there from. For this purpose, business units will retain the right to verify the records maintained by the client cooperative banks/ societies for compliance with the extant instructions on KYC and AML under such arrangements.

In this regard, Urban Cooperative Banks (UCBs) are to utilize the 'at par' cheque facility only for the following purposes:

(a) For their own use.

(b) For their account holders who are KYC complaint provided that all transactions of Rs.50, 000/- or more should be strictly by debit to the customer's account.

(c) For walk-in customers against cash for less than Rs.20, 000/- per individual.

In order to utilize the 'at par' cheque facility in the above manner, UCBs to maintain the following:

(a) Records pertaining to issuance of 'at par' cheques covering inter alia applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque.

(b) Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments.

(c) UCBs to also ensure that all 'at par' cheques issued by them are crossed 'account payee' irrespective of the amount involved

(ii) Customer Data Enrichment

Customer data enrichment in CBS should be a continuous process. Customer information like PAN No., Identification No. Passport No., Driving License No., Mobile/ Telephone No., income details, business type, profession/occupation type, etc. should be updated in the CBS.

(iii) Operation of bank accounts & money mules

a) "Money Mules" can be used to launder the proceeds of fraud schemes (e.g., phishing and identity theft) by criminals who gain illegal access to deposit accounts by recruiting third parties to act as "money mules." In some cases these third parties may be innocent while in others they may be having complicity with the criminals.
b) In a money mule transaction, an individual with an account is recruited to receive cheque deposits or wire transfers and then transfer these funds to accounts held on behalf of another person or to other individuals, minus a certain commission payment. Money mules may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. When caught, these money mules often have their accounts suspended, causing inconvenience and potential financial loss, apart from facing likely legal action for being part of a fraud. Many a times the address and contact details of such mules are found to be fake or not up to date, making it difficult for enforcement agencies to locate the account holder.
c) Regulatory authority has warned that the "Account Lending" activity may be going on in many states. This mechanism may be used by terror outfits and individuals by using other's accounts for transferring funds or making transactions so that they could not be monitored and caught. The original account holder receives rent for this purpose."
d) Business Units should follow the guidelines on KYC / AML / CFT while opening of accounts and monitoring of transactions for reporting STR's to thwart attempts of such criminals to intrude into the banking system.

(iv) Issue of Demand Drafts, etc, for more than Rs.20, 000/-

Business units will ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travelers' cheques for value of Rs.20,000/- and above is effected by debit to the customer's account or against cheques and not against cash payment.

Business Units will not make payment of cheques/drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.

(v) Selling Third party products

When bank sells third party products as agent, the responsibility for ensuring compliance with KYC / AML / CFT regulations lies with the third party. However, to mitigate reputational risk to bank and to enable a holistic view of a customer's transactions, Business Units are advised as follows:

(a) While selling third party products like Insurance/Mutual funds etc. as agents, Business Unit shall verify the identity and address of the walk-in customer.
(b) Business Unit shall also maintain transaction details with regard to sale of third party products and related records for a period of five years
(c) Sale of third party products by Business Units as agents to customers, including walk-in customers, shall be
    i) By debit to customers' account or against cheques and

ii) Obtention & verification of the PAN given by the account based as well as walk-in customers.

This instruction would also apply to sale of bank's own products, payment of dues of credit cards / sale and reloading of prepaid / travel cards and any other product for Rs. 50,000/- and above.

(vi) Secrecy Obligations and Sharing of Information:

(a) Banks shall maintain secrecy regarding the customer information which arises out of the contractual relationship between the banker and customer.

(b) Information collected from customers for the purpose of opening of account shall be treated as confidential and details thereof shall not be divulged for the purpose of cross selling, or for any other purpose without the express permission of the customer.

(c) While considering the requests for data / information from Government and other agencies, banks shall satisfy themselves that the information being sought is not of such a nature as will violate the provisions of the laws relating to secrecy in the banking transactions.

(d) The exceptions to the said rule shall be as under:

i. Where disclosure is under compulsion of law

ii. Where there is a duty to the public to disclose,

iii. the interest of bank requires disclosure and

iv. Where the disclosure is made with the express or implied consent of the customer.

vii) Quoting of PAN

Permanent account number (PAN) of customers shall be obtained and verified while undertaking transactions as per the provisions of IT rule 114B applicable to banks, as amended from time to time. Form 60 shall be obtained from persons who do not have PAN.

In case of existing customers, Business Unit shall obtain the Permanent Account Number (PAN) or Form No.60, failing which Bank shall temporarily cease operations in the account till the time the Permanent Account Number (PAN) or Form No. 60 is submitted by the customer.

Provided that before temporarily ceasing operations for an account, the Business Unit shall give the client an accessible notice and a reasonable opportunity to be heard.

Provided further that if a customer having an existing account-based relationship with the bank gives in writing to the Business Unit that he does not want to submit his Permanent Account Number (PAN) or Form No.60, Business Unit shall close the account and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the customer by obtaining the identification documents as applicable to the customer.

Explanation - For the purpose of this Section, "temporary ceasing of operations" in relation an account shall mean the temporary suspension of all transactions or activities in relation to that account by the bank till such time the customer complies with the provisions of this Section. In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

(viii) Structure of Valid PAN Number

In order to weed out fake PAN submitted by Constituents while account opening or KYC Updation the semantics behind the formation of the 10 digit PAN number is indicated below, for its early identification by the Operating officials. PAN is a 10 digit alpha-numeric number in which the first five characters are alphabets, next four characters are numbers and the last character is again an alphabet. Each character in PAN has its own meaning which has been explained below:

Format: [X X X] [S] [F] 0 0 0 0 [C]

[1 2 3] [4] [5] 6 7 8 9 [10]

The Permanent Account Number has been divided into five groups as:

1) "XXX" - The first three characters are the normal alphabetic series starting from AAA and running up to ZZZ.
2) "S" - The fourth character represents the status of the PAN card holder. It is one of the most important character in Pan Card number and those who deal in PAN cards usually look at this character only to identify the status. The fourth character in PAN can be any of the following. If the fourth character is any alphabet or character other than the following or does not correspond to the status / constitution of the holder, it shall give rise to suspicion that the PAN is fake:

   C - represents a Company

   P - represents a Person

   H - stands for Hindu Undivided Family

   F - represents a Firm

   A - stands for Association of Persons

   T - represents a Trust

   B - represents Body of Individuals

   L - stands for Local Authority

   J - stands for Artificial Juridical Person

   G - stands for Government

3) "F" - The fifth character represents the first character of the PAN holder's Surname (Last name). For eg- If the name of the holder name is say Vishal Bhat, then the fifth character of your PAN will be 'B'.

4) "0000" - The next four characters are again the normal sequential numbers starting from 0001 and running up to 9999.

5) "C" - The last character in the PAN is an alphabetic check digit used as a check-sum to verify the validity of that current code.

7.0 Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures:

Business Units can effectively control and reduce the risk only if they have an understanding of the normal and reasonable activity of the customer so that they have the means of identifying transactions that fall outside the regular pattern of activity. However, the extent of monitoring will depend on the risk sensitivity of the account. Business Unit shall pay special attention to -

(i) All complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

(ii) Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the Business Unit.

(iii) Very high account turnover inconsistent with the size of the balance maintained shall indicate that funds are being 'washed' through the account.

(iv) High-risk accounts shall be subjected to intensified monitoring.

(v) Business Units should closely monitor high value transactions in all accounts, taking note of the background of each customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors.

(vi) High risk associated with accounts of bullion dealers (including sub dealers) & jewelers shall be taken into account to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to Financial Intelligence Unit - India (FIU-IND).

(vii) Review of risk categorization of customers shall be carried out once in six months.

(viii) Business Units should closely monitor the newly opened accounts in the initial 6 months of their opening and track the transactions not in line with the profile of the customer.

(ix) There have been increased instances of fictitious offers, where fraudsters are using RBI s corporate logo/name or any other reputed company in their e-mail messages to convince the victims of the authenticity of the purported messages conveying lottery/prize winning. The fraudsters persuade victims into making initial payment in a specified bank account towards the charges for clearance of the prize money. Whenever such instances are noticed, Business Units should make all efforts to educate the customers and sensitize them over the issue.

(x) Wherever request is received for change in Mobile number, loss of SIM Card, complaints of sudden inactivation or failure of mobile connection, Business Unit should subject such accounts to enhanced monitoring and multiple checks, including calling on such mobile number/land line number seeking confirmation through other modes like e-mail etc.

(xi) The alerts generated by KYC/AML Department, CHQ shall be forwarded to Business Units via e-mail. Business units shall ensure that the alerts so generated on the accounts forwarded via e-mail are consistent with the profile of the customer and report suspicion, if any, to Money Laundering Reporting Officer (MLRO) Vice President (S&C) of their zone who in turn shall report it to Principal Officer. Business Units should go through the alert reports forwarded on regular basis to ensure that the transactions taken place are in conformity with their understanding/knowledge of the customer and his/her activity, means and worth etc. Wherever necessary, Business Unit should seek clarification from the customer and get satisfied with the genuineness of the transaction. Transaction of suspicious nature should immediately be reported to concerned MLRO of their Zone. The Business Units shall further ensure that Enhanced Due Diligence is carried for all those accounts (alerts raised) including the ones perceived as high risk accounts by them.

(xii) Any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travelers cheques for value of above Rupees Twenty thousand should be effected by debit to the customer's account or against cheques and not against cash payment.

(xiii) Business Units are advised to mandatorily obtain either PAN or Form 60/61 (if PAN is not available) for opening of accounts and also at the time of accepting cash receipt for Rs. 50,000/- and above. If the customer appears to be structuring the transactions into a serious of transactions below the threshold of Rs.50,000/-, Business Units are required to obtain PAN or Form 60/61 (if PAN is not available) from the customer and also consider filling of an STR if warranted.

(xiii) Accounts of multi-level marketing (MLM) companies: It has been observed that accounts of Multi-level Marketing (MLM) Companies were misused for defrauding public by luring them into depositing their money with the MLM Company by promising a high return. Such depositors are assured of high returns and issued post-dated cheques for interest and repayment of principal. So long as money keeps coming into the MLM company's account from new depositors, the cheques are honored but once the chain breaks, all such post-dated instruments are dishonored. This results in fraud on the public and is a reputational risk for the Bank concerned. Business Unit shall closely monitor the transactions in accounts of marketing firms. In cases where a large number of cheque books are sought by the company, there are multiple small deposits (generally in cash) across the country in one bank account and where a large number of cheques are issued bearing similar amounts / dates, the Business Unit shall carefully analyze such data and in case they find such unusual operations in accounts, the matter shall be immediately reported to Reserve Bank and other

appropriate authorities such as Financial Intelligence Unit India (FIU-India).

Keeping in view of the above, Business Units should ensure as under:

(i) Strict adherence to the KYC/AML guidelines issued from time to time relating to opening of accounts, risk categorization of accounts and monitoring of transactions in accounts.

(ii) The transactions that are deviating from the threshold limit/ outside the normal transaction region should be probed into.

(iii) Closely monitor newly opened accounts in the initial 6 months and due diligence to be applied to transactions not in line with the customer profile.

(iv) Staff members in the Front line/ operations desks should remain vigilant to handle queries from customers regarding such lottery winnings where the customers have been advised to deposit money in specified accounts.

8.0 Risk Management

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

- Reputational Risk

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

- Compliance Risk

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

- Operational Risk

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

- Legal Risk

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

Bank will exercise ongoing due diligence with respect to the business relationship with every client and closely examine the transactions in order to ensure that they are consistent with its knowledge about the clients, their business and risk profile and where necessary, the source of funds.

8.2 Roles and Responsibilities for KYC/AML Standards

The basic KYC document check shall be done by the authorized Business Unit officials at the Business Unit level for all accounts. For High Risk customers, in addition to the authorized Business Unit officials, the Business Unit Head shall verify the KYC.

(The Board of Directors of the bank is responsible and committed to ensure that an effective KYC program is put in place in the bank by establishing appropriate procedures and to ensure their

effective implementation to achieve full compliance of KYC/AML/CFT guidelines of RBI in letter and spirit.)

The Machinery for implementing the KYC Programme consists of:

Designated Director (Chairman & CEO)

- Ensure overall compliance with the obligations imposed under Chapter IV and Sec.12 of PML Amendment Act 2010
- Oversight of implementation of the policies formulated by the Board
- Liaisoning with Director FIU-IND

AML Principal Officer

- Monitoring the implementation of the bank's KYC/AML policy.
- Maintaining liaison with law enforcement agencies
- Ensuring submission of periodical Reports to the top Management/board.
- Oversight of timely submission of reports to FIU-IND viz., CTR, STR, CCR, NTR, Cross Border Wire transfers >5 lacs etc
- Formulation of Proper systems, procedures and Controls in the KYC/AML area

Central AML Cell

- Transaction Monitoring through AML application
- Maintenance and development/customization of AML application in liaison with bank's IT team and the system Vendor
- Timely submission of reports to FIU-IND Viz., CTR, STR, CCR, NTR, Cross Border Wire transfers >5 lacs etc.
- KYC/AML Inspection Reports

Supervision & Control Department

Conducting Regular, Concurrent and Special KYC audits.

Zonal Offices:

- Oversight of compliance of KYC/AML guidelines by Business Units
- Following up and ensuring full rectification of deficiencies in KYC/AML compliance reported in various Inspections.

Compliance Function

- Evaluating and ensuring adherence to the KYC policies and procedures (based on Bank's KYC policy)
- Independent evaluation of the bank's own KYC/AML/CFT policies and procedures vis-à- vis legal and regulatory requirements

8.3 Employee Training

Bank will ensure to have an ongoing employee training program so that the members of staff are adequately trained in AML/CFT policy. The focus of the training should be different for frontline staff, compliance staff and staff dealing with new customers. The front desk staff needs to be specially trained to handle issues arising from lack of customer education. It shall be ensured that the audit function of the bank is properly staffed with persons adequately trained and well-versed in AML/CFT policies of the bank, regulation and related issues.

8.4 Hiring of Employees

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

9.0 Intra-Bank Deposit Accounts Portability

Intra-Bank Deposit account portability shall be applicable for Savings and Current accounts only. The procedural guidelines, with regard to KYC/AML, to be followed by operative levels for transfer of accounts from one Business Unit to another Business Unit (intra-bank) shall be as under:

9.1 The process of transferring the account of the customer under account portability shall be initiated by the base Business Unit (transferor Business Unit) only i.e. the Business Unit where the party is presently maintaining the account. The transferor Business Unit shall receive a formal request under the recorded signatures of the customer along with the unused cheque leave/s.

9.2 The transferor Business Unit, before transferring of account, will ensure that the account is fully KYC compliant and no other irregularity is noticed in the account. In case the account is Non-KYC compliant, the KYC Compliance shall mandatorily be ensured by the transferor Business Unit prior to its transfer to the transferee Business unit. Periodical updations of KYC data, if due, as per existing guidelines has to be ensured by the transferor Business Unit prior to its transfer. After obtaining necessary KYC documents, the transferor Business Unit shall update the same in option CUMM (Field free code 1 = "KYC"). A system check has also been placed in finacle to restrict transfer of accounts where KYC requirement has not been complied with.

9.3 The transferor Business Unit shall also physically transfer all KYC documents obtained from the customer, along with Account Opening Form, Specimen Signature Card etc, mentioning the date of transfer under seal & signature of Business Unit Head/ Authorized Officer. The transferor Business Unit shall keep a copy of the documents transferred to the transferee Business Unit properly in "accounts transferred file".

9.4 KYC verification once done by one Business Unit of the Bank shall be valid for transfer of the account to any other Business Unit of the Bank, provided full KYC verification has already been done for the concerned account and the same is not due for periodic updation.

10.0 Record Management

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

i) Maintenance of records of transactions

ii) Information to be preserved

iii) Maintenance and preservation of record

iv) Reporting to Financial Intelligence Unit – India

10.1 Maintenance of records of transactions

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

a) All cash transactions of the value of more than Rs. 10.00 lacs or its equivalent in foreign currency.

b) All series of cash transactions integrally connected to each other, which have been valued below Rs.10.00 lacs or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rs.10.00 lacs.

c) All transactions involving receipts by non-profit organizations of value more than rupees ten lacs or its equivalent in foreign currency.

d) All cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or documents has taken place facilitating the transactions.

e) All suspicious transactions whether or not made in cash and by way of cheques including third party cheques, pay orders, demand drafts, cashier cheques, travelers cheques, account transfers, credits or debits into or from any non-monetary accounts (shares, demat accounts), money transfer or remittance, loans and advances, collection services etc.

10.2 Information to be preserved

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

a) The nature of the transaction.

b) The amount of transaction and the currency in which it was denominated.

c) The date on which the transaction was conducted and

d) The parties to the transaction.

11.0 Maintenance and Preservation of record

11.1 Records containing information of all transactions including the records of transactions detailed in Rule 3 has to be maintained.

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

11.3 Records pertaining to the identification of the customer and his address (e.g. copies of documents like passports, identity cards, driving licenses, PAN card, utility bills etc.) Obtained while opening the account and during the course of business relationship are properly preserved for at least five years after the business relationship is ended as required under Rule 10 of the Rules ibid. The identification records and transaction data should be made available to the competent authorities upon request.

11.4 Business Units shall pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose and purpose thereof should, as far as possible, be examined and the findings at business units as well as Principal Officer level to be properly recorded. Such records and related documents to be made available to help auditors in their day-to-day work relating to scrutiny of transactions and other relevant authorities. These records are required to be preserved for five years as is required under PMLA, 2002.

12.0 Reporting to Financial Intelligence Unit – India

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

The formats in which the transactions are to be reported are:

i) Cash Transactions Report (CTR);
ii) Suspicious Transactions Report (STR);
iii) Counterfeit Currency Report (CCR);
iv) Non-Profit Organization Transaction Report (NTR);

12.2 Cash and Suspicious Transaction Reports

12.3 Cash Transaction Report (CTR)

The Prevention of Money-laundering Act, 2002, and the rules there under require every banking company to furnish to FIU-IND, Cash Transaction Report (CTR) which shall include:

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds rupees ten lakhs or its equivalent in foreign currency.

For filling Cash Transaction Report (CTR), the following instructions shall be adhered to:

i) The Cash Transaction Report (CTR) for each month shall be submitted to FIU-IND by 15th of the succeeding month.

ii) The details of individual transactions below Rupees Fifty thousand need not to be furnished.

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

iv) A summary of cash transaction report for the Bank as a whole should be compiled by the Principal Officer every month as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

v) Cash Transaction Reports (CTR) shall be submitted centrally by KYC/AML Department to FIU-INDIA.

vi) The Cash Transaction Reports (CTR) so generated and reported to FIU-IND shall be available on Bank's Finacle Home Page under the head "CTR Reports". The Business Unit Head shall download the report pertaining to their Business Unit and ensure Enhanced Due Diligence (EDD) for all such accounts which have been reported in the CTR. The suspicion, if any, observed shall be reported to Money Laundering Reporting Officer (MLRO) of their respective zone for onward submission to Principal Officer.

12.4 Counterfeit Currency Report

All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by Business Units to Principal Officer directly enabling him to submit the report to FIU-IND in the specified format by the 15th day of the succeeding month (Counterfeit Currency Report – CCR). These cash transactions should also include transactions where forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

12.5 Suspicious Transaction Report (STR)

For Suspicious Transaction Report (STR), the following instructions shall be adhered to:

i) For determination of suspicious transactions, necessary guidance shall be taken from the definition of suspicious transaction contained in PMLA Rules as amended from time to time.
ii) In some cases, transactions may be abandoned /aborted by customers on being asked to give some details or to provide documents. All such attempted transactions should be reported in STRs, even if not completed by customers, irrespective of the amount of the transaction.
iii) STRs shall be made if there are reasonable ground to believe that the transaction involve proceeds of crime generally irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences in part B of Schedule of PMLA, 2002.
iv) The Suspicious Transaction Report (STR) shall be furnished within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer shall record his / her reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a Business Unit or any other office. Such report should be made available to the competent authorities on request.
v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, the indicative list of suspicious activities contained in IBA's Guidance Note for Banks, 2011' may be relied upon. The same is placed as Annexure- IV to this policy.
vi) The operative levels shall submit the Suspicious Transaction Report as and when it is detected.
vii) No restrictions shall be put on operations in the accounts where an STR has been made. The fact of

furnishing of STR shall be kept strictly confidential, as required under PML Rules. Customer shall not be tipped off at any level.

12.6 Non-Profit Organization Report (NTR)

As per the prevention of Money-Laundering Act 2002, the "Non-Profit-Organizations" means any entity or organization that is registered as a trust or a society under the societies Registration Act, 1860 or any similar state legislation or a company registered under Section 8 of the Companies Act, 2013.

The Business Units shall incorporate the relevant CONSTITUTION fields of all such accounts available in CUMM (Customer Master Maintenance):

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

12.7 Cross Border Wire Transfer

Cross-border Wire Transfer Report (CWTR) is required to be filed by 15th of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency during a month where either the origin or destination of fund is in India.CWTR report shall be submitted centrally by KYC/AML deptt. every month to FIU-India as per the schedule. AD business unit shall ensure that the counter party details of the sender/beneficiary of the CWTR transaction are invariably punched in the customized fields of IRM/ORM/FBM menu options of CBS.

13.0 Correspondent Banking

13.1 Correspondent banking is the provision of banking services by one bank (the 'correspondent bank') to another bank (the 'respondent bank'). These services may include cash/funds management, international wire transfers, drawing arrangements for demand drafts and mail transfers, payable-through-accounts, cheques clearing, etc. The bank while entering into any kind of correspondent banking arrangement 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 correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country shall be of special relevance. Similarly, the bank shall also 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 only with the prior approval of the Board. The Board may in the alternative delegate powers in this regard to a committee headed by the Chairman/CEO of the bank and lay down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent 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.

13.2 Bank shall not enter into a correspondent relationship with a 'shell bank'. A Shell bank is a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group. "Shell banks" are not permitted to operate in India. Bank shall also guard against establishing relationships with respondent foreign financial institutions that permit their accounts to be used by "shell banks". The Bank shall move cautiously 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. The bank shall ensure that the respondent bank have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts

14.0 Wire Transfer

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

14.2 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.

14.3 Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit - India (FIU-IND) for analyzing 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, it shall be ensured by business units that all wire transfers are accompanied by the following information:

14.4 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.

14.5 Domestic wire transfers

i) Information accompanying all domestic wire transfers of Rs50000/- (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 business unit 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 business unit must insist on complete customer identification before effecting the transfer. In case of non cooperation from the customer, efforts should be made to establish his identity and Suspicious Transaction Report (STR) should be submitted as per the prescribed procedure.

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

14.6 Exemptions

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

15.0 Role of Ordering, Intermediary and Beneficiary banks

15.1 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 five years.

15.2 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 five years (as required under Prevention of Money Laundering Act, 2002) by the receiving intermediary bank of all the information received from the ordering bank.

15.3 Beneficiary bank

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

16.0 Combating Financing of Terrorism

The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC). The Bank will ensure before opening the account that the name(s) of the proposed customer does not appear in the lists of designated/banned individuals/entities circulated by RBI/Bank from time to time.

(a) The "ISIL (Da'esh) & Al-Qaida Sanctions List", includes names of individuals and entities associated with the Al-Qaida. The Updated Al-Qaida Sanctions List is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/al-qaida-r.xsl.

(b) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities (Section B) associated with the Taliban which is available at https://scsanctions.un.org/fop/fop?xml=htdocs/resources/xml/en/consolidated.xml&xslt=htdocs/resources/xsl/en/taliban-r.xsl.

The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and Bank to update the lists and take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967.

Bank will also scan all the existing accounts to ensure that no account is linked to any of the individuals/entities in the list. In case the full details of accounts bearing resemblance with any of the individuals/entities in the list, KYC-AML Department CHQ shall report the same to FIU-IND apart from advising Ministry of Home Affairs as required under UAPA notification dated August 27, 2009.

In addition to the above, other UNSC resolutions circulated by the Reserve Bank in respect of any other jurisdictions / entities from time to time shall also be taken note of (including the latest list of UNSC resolution on Democratic People's Republic of Korea – DPRK).

17.0 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 March 14, 2019 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) It shall be ensured that the procedure laid down in the UAPA Order dated March 14, 2019 (Annexure V) is strictly followed in order to ensure meticulous compliance to the Order issued by the Government. The reporting shall be made through the Principal Officer of the Bank.

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

iv) In terms of Para 4 of the Order, in regard to funds, financial assets or economic resources or related services held in the form of bank accounts, the RBI would forward the designated lists to the banks requiring them to:

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

b) In case, the particulars of any of the customers match with the particulars of designated individuals/ entities, the Bank shall immediately, not later than 24 hours from the time of finding out such customer, inform full particulars of the funds, financial assets or economic resources or related services held in the form of bank accounts, held by such customer on their books to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail:

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

d) Bank shall also send a copy of the communication mentioned in (b) above to the UAPA nodal officer of the state/UT where the account is held as the case may be and to FIU-India.

e) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the Bank would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on 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 not exceeding 5 working days from the date of receipt of such particulars.

b) In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned Bank Business Unit under intimation to Reserve Bank of India and FIU-IND.

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

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

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

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

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

d) Upon receipt of the requests from the UAPA nodal officer of ISI Division, the list would be forwarded to banks and the procedure as enumerated at paragraphs 3 [(i), (ii), (iii), and (iv) shall be followed.

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

vii) Procedure for unfreezing of funds, financial assets or economic resources or related services of individuals/ entities inadvertently affected by the freezing mechanism upon verification that the person or entity is not a designated person. Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank. The banks shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph (iv)(b) above within two working days. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within fifteen working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

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

18.0 Jurisdictions that do not or insufficiently apply the FATF Recommendations

18.1 Risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement shall be taken into account. In addition to FATF Statements circulated by Reserve Bank of India from time to time, 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.

18.2 All forex designated Business units 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. The suspicious transaction report shall be filed where ever deemed fit as per the prescribed procedure.

19.0 Principal Officer

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

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

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

20.0 Designated Director

Bank is required to nominate a Director on its Board as "Designated Director", as per the provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure overall compliance with the obligations under the Act and Rules.

20.1 Compliance of KYC policy

(a) For the purpose of determining compliance of this policy, it shall be ensured that decision-making functions of compliance with KYC norms are not outsourced.

Annexure-I

Cross Reference(s)

1. Section 5.3 (iii) Customer Acceptance Policy
2. Section 6.1 Customer Due Diligence
3. Section 6.1.1 Customer Due Diligence (CDD) Procedure for Individuals

Customer Identification Procedure

Documents to be obtained from customers.

Types of Customers	Description of Documents
Accounts of Individuals -Proof of Identity and Address	<u>Certified copy of any one of the following officially valid document [Copy verified from the original will be kept on record with AOF]</u> 1. The passport 2. The driving licence 3. Proof of possession of Aadhaar number (in such form as are issued by the Unique Identification Authority of India) 4. The Voter's Identity Card issued by the Election Commission of India 5. Job card issued by NREGA duly signed by an officer of the State Government and 6. Letter issued by the National Population Register containing details of name and address. Where 'simplified measures' are applied for verifying the identity of customers (low risk categorized 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, Statutary / 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. Where 'simplified measures' are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be 'officially valid documents' (OVDs) provided that the OVD updated with current address is submitted within 3 months.: (i) Utility bill which is not more than two months old of any service provider (electricity, telephone, postpaid mobile phone, piped gas, water bill); (ii) Property or Municipal Tax receipt; (iii) Bank account or Post Office savings bank account statement; (iv) Pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (v) Letter of allotment of accommodation from employer issued by State or Central Government departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions and listed companies. Similarly, leave and license agreements with such employers allotting official accommodation; and (vi) Documents issued by Government departments of foreign jurisdictions and letter issued by Foreign Embassy or Mission in India. Note: A customer is required to submit only one OVD for both proof of identity and for proof of address as part of KYC procedure. If the OVD for proof of identity does not have the proof of address (for e.g. PAN Card), then the customer is required to submit another OVD for proof of address.

Accounts of sole proprietary firms - Proof of the name, address and activity of the concern & the proprietor	In addition to KYC documents of the Proprietor, certified copies of any two of the following documents as proof of business /activity in the name of the proprietary firm shall be obtained: (a) Registration certificate (b) Certificate / licence issued by the municipal authorities under Shop and Establishment Act. (c) Sales and income tax returns. (d) CST / VAT / GST certificate (provisional / final). (e) Certificate / registration document issued by Sales Tax / Service Tax / Professional Tax authorities. (f) IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT or Licence / certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated / acknowledged by the Income Tax authorities. (h) Utility bills such as electricity, water, landline telephone bills. Note: However, in cases where the Bank is satisfied that it is not possible to furnish two such documents in the name of proprietary concern, the Bank may accept only one of the above mentioned documents as activity proof provided that the Bank undertakes contact point verification, collects such information as is required to establish the existence of such firm, confirms, clarifies and satisfies itself that the business activity is verified from the address of the proprietary concern.
Accounts of Companies - Name of Company, Principal Place of business (registered Address), Mailing Address of the company, Telephone/ fax Number	In addition to KYC documents of the Directors of the company, certified copies of the following documents should be obtained: Certificate of incorporation **a)** Memorandum and Articles of Association **b)** Copy of Permanent Account Number (PAN) in the name of the company duly validated in PAN/TAN application of the bank. **c)** A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf. **d)** KYC Documents of the managers, officers or employees holding an attorney to transact on the company's behalf, as the case may be, are required as applicable to accounts of Individuals stated above.
Accounts of Partnership firms - Legal name, Address, Name of all partners and their addresses, Telephone number of the firm and partners	In addition to KYC documents of all partners, certified copies of the following documents shall be obtained: **a)** Registration certificate **b)** Partnership deed **c)** Copy of Permanent Account Number (PAN) in the name of the partnership firm duly validated in PAN/ TAN application of the bank. **d)** KYC Documents of the person holding an attorney to transact on the behalf of the firm are required as applicable to accounts of Individuals stated above.
Accounts of Trusts - Name of trustees, settlors, beneficiaries and signatories as applicable, Name and address of the founder, the manager/ directors and the beneficiarie, Telephone/fax numbers	In addition to KYC documents of the Managing Trustees/ Founders/ Managers/ Directors, certified copies of the following documents of the Trust are to be obtained: a) Registration certificate b) Trust deed c) Copy of Permanent Account Number (PAN) in the name of the Trust duly validated in PAN/TAN application of the bank or Form No. 60. d) KYC Documents of the person holding an attorney to transact on the behalf of the firm are required as applicable to accounts of Individuals stated above.

Accounts of unincorporated association or a body of individuals	In addition to KYC documents of the Founders/Managers/ Directors and their addresses, certified copies of the following documents shall be obtained: (a) Resolution of the managing body of such association or body of individuals (b) Copy of Permanent Account Number (PAN) in the name of the unincorporated association or a body of individuals duly validated in PAN/TAN application of the bank or Form No.60. (c) Power of attorney granted to transact on its behalf (d) KYC Documents of the person holding an attorney to transact on its behalf are required as applicable to accounts of Individuals stated above, and (e) Such information as may be required by the Bank to collectively establish the legal existence of such an association or body of individuals. Note: 1. Unregistered trusts/ partnership firms shall be included under the term 'unincorporated association'. 2. Term 'body of individuals' includes societies.
Accounts of Hindu Undivided Family	In addition to KYC documents of Karta and Major Co-parceners, the following documents should be obtained: • Recent Passport Photographs duly self attested by Karta and major co-parceners. • Declaration of HUF and its Karta • Names and addresses of Karta and Major Co-parceners. • An officially valid document in respect of the person holding an attorney to transact on its behalf.
Accounts of Government Authorities	For opening accounts of juridical persons not specifically covered in the earlier part, such as Government or its Departments, societies, Universities and local bodies like village panchayats, a certified copy of the following documents shall be obtained:- (a) Document showing name of the person authorized to act on behalf of the entity; (b) Documents of the person holding an attorney to transact on its behalf are required as applicable to accounts of Individuals stated above. and (c) Such Documents which may establish the legal existence of such an entity/juridical person.

Annexure - I (A)

Cross Reference(s)

1. Section 6.1.4 (F) Simplified KYC norms for Foreign Portfolio Investors (FPIs), above

KYC documents for eligible FPIs under PIS

		FPI Type		
	Document Type	Category I	Category II	Category III
Entity Level	Constitutive Documents (Memorandum and Articles of Association, Certificate of Incorporation etc.)	Mandatory	Mandatory	Mandatory
	Proof of Address	Mandatory (Power of Attorney {PoA} mentioning the address is acceptable as address proof)	Mandatory (Power of Attorney mentioning the address is acceptable as address proof)	Mandatory other than Power of Attorney
	PAN	Mandatory	Mandatory	Mandatory
	Financial Data	Exempted *	Exempted *	Mandatory
	SEBI Registration Certificate	Mandatory	Mandatory	Mandatory
	Board Resolution (FPIs from certain jurisdictions where the practice of passing Board Resolution for the purpose of opening bank accounts etc. is not in vogue, may submit 'Power of Attorney granted to Global Custodian/Local Custodian in lieu of Board Resolution')	Exempted *	Mandatory	Mandatory
Senior Management (Whole Time Directors/ Partners/ Trustees/ etc.)	List	Mandatory	Mandatory	Mandatory
	Proof of Identity	Exempted *	Exempted *	Entity declares* on letter head full name, nationality, date of birth or submits photo identity proof
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

Authorized Signatories	List and Signatures	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory - list of Global Custodian signatories can be given in case of PoA to Global Custodian	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *
Ultimate Beneficial Owner (UBO)	List	Exempted *	Mandatory (can declare "no UBO over 25%")	Mandatory
	Proof of Identity	Exempted *	Exempted *	Mandatory
	Proof of Address	Exempted *	Exempted *	Declaration on Letter Head *
	Photographs	Exempted	Exempted	Exempted *

* Not required while opening the bank account. However, FPIs concerned may submit an undertaking that upon demand by Regulators/Law Enforcement Agencies the relative document/s would be submitted to the bank.

Category		Eligible Foreign Investors
I.		Government and Government related foreign investors such as Foreign Central Banks, Governmental Agencies, Sovereign Wealth Funds, International/ Multilateral Organizations/ Agencies.
II.	a)	Appropriately regulated broad based funds such as Mutual Funds, Investment Trusts, Insurance /Reinsurance Companies, Other Broad Based Funds etc.
	b)	Appropriately regulated entities such as Banks, Asset Management Companies, Investment Managers/ Advisors, Portfolio Managers etc.
	c)	Broad based funds whose investment manager is appropriately regulated.
	d)	University Funds and Pension Funds.
	e)	University related Endowments already registered with SEBI as FII/Sub Account.
III.		All other eligible foreign investors investing in India under PIS route not eligible under Category I and II such as Endowments, Charitable Societies/Trust, Foundations, Corporate Bodies, Trusts, Individuals, Family Offices, etc.

Annexure-II

Cross Reference(s)

1. Section 5.4(IV)(C) Customer Risk Categorization
2. Section 5.4(V) Roles & Responsibilities of Business Units

Alert Indicators for Business Units

S.No	Alert Indicator	Indicative Rule/Scenario
1	Customer left without opening account.	• Customer did not open account after being informed about KYC requirements.
2	Customer offered false or forged identification documents.	• Customer gives false identification documents or documents that appear to be counterfeited, altered or inaccurate.
3	Identity documents are not verifiable.	• Identity documents presented are not verifiable i.e, Foreign documents etc.
4	Address found to be nonexistent.	• Address provided by the customer is found to be nonexistent.
5	Address found to be wrong.	• Customer not staying at address provided during account opening.
6	Difficult to identify beneficial owner.	• Customer uses complex legal structures or where it is difficult to identify the beneficial owner.
7	Customer is being investigated for ML offences.	• Customer has been the subject of inquiry from any law enforcement agency relating to Money Laundering.
8	Adverse media report received about the customer.	• Match of customer details with persons reported in local media/ open source for money laundering /financing for illegal activities.
9	Customer did not complete transaction.	• Customer did not complete transaction after queries about source of funds etc.
10	Customer is nervous.	• Customer is hurried or nervous.
11	Customer is over cautious.	• Customer over cautious in explaining genuineness of the transaction.
12	Customer provides inconsistent information.	• Customer changes the information provided after more detailed information is requested. • Customer provides information that seems minimal, possibly false or inconsistent.
13	Customer acting on behalf of a third party.	• Customer has vague knowledge about amount of money involved in the transaction. • Customer taking instructions for conducting transactions. • Customer is accompanied by unrelated individuals.
14	Multiple customers working as a group.	• Multiple customers arrive together but pretend to ignore each other.

15	Customer avoiding near Business Units.	• Customer travels unexplained distances to conduct transactions.
16	Customer offers different identifications on different occasions.	• Customer offers different identifications on different occasions with an apparent attempt to avoid linkage of multiple transactions.
17	Customer wants to avoid reporting.	• Customer makes inquiries or tries to convince staff to avoid reporting.
18	Customer could not explain source of funds.	• Customer could not explain source of funds satisfactorily.
19	Transaction is unnecessarily complex.	• Transaction is unnecessarily complex for its stated purpose.
20	Transaction has no economic rationale.	• The amounts or frequency or the stated reason of the transaction does not make sense for the particular customer.
21	Transaction inconsistent with the business.	• Transaction involving movement of funds which is inconsistent with the customers' business.
22	Unapproved inward remittance in NPO.	• Foreign remittance received by NPO not approved by FCRA.
23	Alert raised by agent.	• Alert raised by agents about suspicion.
24	Alert raised by other institution.	• Alert raised by other institutions, subsidiaries or business associates including cross-border referral.
25	Complaint received from public	• Complaint received from public for abuse of account for committing fraud etc.
26	Customer is being investigated for criminal offences.	• Customer has been subject of inquiry from any law enforcement agency relating to criminal offences.

Annexure-III

Cross Reference(s)

1. Section 5.4 (III) Risk Perception in respect of Customer
2. Section 5.4(V) Roles & Responsibilities of Business Units

APPENDIX – A

List of Low/Medium/High risk Customers based on the recommendations of IBA Working Group.		
Low Risk	Medium Risk	High Risk

1. Cooperative Bank 2. Ex-staff, Govt./ Semi Govt. Employees 3. Illiterate 4. Individual 5. Local Authority 6. Other Banks 7. Pensioner 8. Public Ltd. 9. Public Sector 10.Public Sector Bank 11.Staff. 12.Regional Rural Banks 13.Govt./Semi-Govt. Local Body 14.Cooperative Society 15.Senior Citizens 16.Self Help Groups	1. Gas Station 2. Car / Boat / Plane Dealership 3. Electronics (wholesale) 4. Travel agency 5. Used car sales 6. Telemarketers 7.Providers of telecommunications service, internet café, IDD call service, phone cards, phone center 8. Dot-com company or internet business 9. Pawnshops 10.Auctioneers 11.Cash-Intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc. 12.Sole Practitioners or Law Firms (small,little known) 13.Notaries (small,little known) 14.Secretarial Firms (small, little known) 15.Accountants (small, little known firms) 16.Venture capital Companies 17.Blind 18.Purdanashin. 19.Registered Body. 20.Corporate Body 21.Joint Sector 22.Partnership 23.Private Bank 24.Private Ltd. Company 25.Unregistered body. 26.Proprietorship.	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 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities 3. Individuals and entities in watch lists issued by Interpol and other similar international organizations 4. Customers with dubious reputation as per public information available or commercially available watch lists 5. Individuals and entities specifically identified by regulators, FIU and other competent authorities as high-risk 6. Customers conducting their business relationship or transactions in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the Customer, frequent and unexplained movement of accounts to different institutions,frequent and unexplained movement of funds between institutions in various geographic locations etc. 7. Customers based in high risk countries/jurisdictions or locations 8. Politically exposed persons (PEPs) of foreign origin, Customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner; 9. Non-resident Customers and foreign nationals 10.Embassies / Consulates 11.Off-shore(foreign) corporation/business 12.Non face-to-face Customers 13.High net worth individuals 14.Firms with 'sleeping partners' 15.Companies having close family shareholding or beneficial ownership 16.Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale 17.Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence 18.Investment Management / Money Management Company/Personal Investment Company 19.Client Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians etc. 20.Trusts, charities, NGOs/NPOs (especially those operating on a"cross-border" basis) unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies) 21.Money Service Business: including seller of: Money Orders / Travelers' Cheques / Money Transmission /Cheque Cashing / Currency Dealing or Exchange 22.Business accepting third party cheques (except supermarkets or retail stores that accept payroll cheques/cash payroll cheques) 23.Gambling/gaming including "Junket Operators" arranging gambling tours 24.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). 25.Customers engaged in a business which is associated with higher levels of corruption (e.g., Arms manufacturers, dealers and intermediaries). 26.Customers engaged in industries that might relate to nuclear proliferation activities or explosives. 27.Customers that may appear to be Multi level marketing companies etc. 28.Customers dealing in Real Estate business (transactions need to be monitored with enhanced due diligence). 29.Associations/Clubs 30.Foreign Nationals. 31.NGO. 32.Overseas Corporate Bodies. 33.Bullion dealers and Jewelers 34.Pooled accounts. 35.Other Cash Intensive business. 36.Shell Banks – Transactions in corresponding banking. 37. Non-Bank Financial Institution 38. Stock brokerage 39. Import / Export 40. Executors/Administrators 41. HUF. 42. Minor.
The above categorization of customers under risk perception is only illustrative and not exhaustive.		

APPENDIX – B

High / Medium Risk Products and Services

Business Units / Offices are required to pay special attention to any money laundering threats that may arise from new or developing technologies including internet banking that might favour anonymity, and take measures, if needed, to prevent their use in money laundering schemes. Presently a variety of Electronic Cards are used by customers for buying goods and services, drawing cash from ATMs, and for electronic transfer of funds. Business Units should ensure that appropriate KYC procedures are duly applied before issuing the Cards including Add-on / Supplementary Cards to the customers.

Indicative list of High / Medium Risk Products and Services

1. Electronic funds payment services such as Electronic cash (e.g., stored value and pay roll cards), funds transfer (domestic and international) etc.

2. Electronic banking

3. Private banking (domestic and international)

4. Trust and asset management services

5. Monetary instruments such as Travelers' Cheque

6. Foreign correspondent accounts

7. Trade finance (such as letters of credit)

8. Special use or concentration accounts

9. Lending activities, particularly loans secured by cash collateral and marketable securities

10.Non-deposit account services such as Non-deposit investment products and Insurance

11.Transactions undertaken for non-account holders (occasional Customers)

12.Provision of safe custody and safety deposit boxes

13.Currency exchange transactions

14.Project financing of sensitive industries in high-risk jurisdictions

15.Trade finance services and transactions involving high-risk jurisdictions

16.Services offering anonymity or involving third parties

17.Services involving banknote and precious metal trading and delivery

18.Services offering cash, monetary or bearer instruments; cross-border transactions, etc.

APPENDIX – C

High / Medium Geographic risk

Business Units/offices are required to prepare a profile for all new customers based on risk categorization, taking into account the location of the customer and the customer's
clients as well as factors such as the nature of business activity, mode of payments, turnover and customer's social and financial status including location of his business activity and to exercise due diligence based on the bank's risk perception. The customer should be subjected to higher due diligence if following criteria falls under "high-risk" geographies

- Country of nationality (individuals)
- Country of residential address (individuals)
- Country of incorporation (legal entities)
- Country of residence of principal shareholders / beneficial owners (legal entities)
- Country of business registration such as Business Unit/liaison/project office.
- Country of source of funds
- Country of the business or correspondence address
- Country with whom customer deals (e.g. 50% of business – trade, etc.)

Apart from the risk categorization of the countries, Business Units/offices should categorize the geographies/locations within the country on both Money Laundering (ML) and Financing Terrorism (FT) risk.

Indicative List of High / Medium Risk Geographies (Countries/Jurisdictions)
1. Countries subject to sanctions, embargos or similar measures in the United Nations Security Council Resolutions ("UNSCR").
2. Jurisdictions identified in FATF public statement as having substantial money laundering and terrorist financing (ML/FT) risks (www.fatf-gafi.org)
3. Jurisdictions identified in FATF public statement with strategic AML/CFT deficiencies (www.fatf-gafi.org)
4. Tax havens or countries that are known for highly secretive banking and corporate law practices
5. Countries identified by credible Sources as lacking appropriate AML/CFT laws, regulations and other measures.
6. Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
7. Countries identified by credible sources as having significant levels of criminal activity.
8. Countries identified by the bank as high-risk because of its prior experiences, transaction history, or other factors (e.g. legal considerations, or allegations of official corruption).

Locations
1. Locations within the country known as high risk for terrorist incidents or terrorist financing activities (e.g. sensitive locations/cities and affected districts)
2. Locations identified by credible sources as having significant levels of criminal, terrorist, terrorist financing activity.
3. Locations identified by the bank as high-risk because of its prior experiences, transaction history, or other factors.

NOTE:
Risk assessment should take into account following risk variables specific to a particular customer or transaction:

- The purpose of an account or relationship
- Level of assets to be deposited by a particular customer or the size of transaction undertaken.
- Level of regulation or other oversight or governance regime to which a customer is subjected to.
- The regularity or duration of the relationship.
- Familiarity with a country, including knowledge of local laws, regulations and rules as well as structure and extent of regulatory oversight.
- The use of intermediate corporate vehicles or other structures that have no apparent commercial or other rationale or increase the complexity or otherwise result in lack of transparency

Annexure-IV

Cross Reference(s)

1. Section 5.4 (III) Risk Perception in respect of Customer
2. Section 5.4(IV)(A) - Customer Risk categorization
3. Section 12.5(V) – Suspicious Transaction Report (STR)

Parameters for Risk Based Transaction Monitoring

"IBA Working Group Report dated March 30, 2011"

Transaction Involving Large Amounts of Cash

1. Exchange an unusually large amount of small denomination notes for those of higher denomination;
2. Purchasing of selling of foreign currencies in substantial amount by cash settlement despite the customer having an account with the bank;
3. Frequent withdrawal of large amount by means of cheques, including traveler's cheques;
4. Frequent withdrawing of large cash amount that do not appear to be justified by the customer's business activity;
5. Large cash withdrawals from a previously dormant/inactive account of from an account which has just received an unexpected large credit from abroad;
6. Company transactions, both deposit and withdrawals, that are denominated by unusually large amount 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, bill of exchange etc;
7. Depositing cash by means of numerous credit slips by a customer such that the amount of cash deposit is not substantial, but the total of which is substantial.

Transactions that do not make Economic Sense

1. A customer having a large number of accounts with the same bank, with frequent transfers between different account;
2. 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.
3. Corporate accounts where deposits or withdrawals are primarily in cash rather than cheques.
4. Corporate account 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.
5. Unusual application for DD/TT/PO against cash.
6. Accounts with large volume of credits through DD/TT/PO whereas the nature of business does not justify such credits.
7. Retail deposit of many cheques but rare withdrawals for daily operations.

Attempts to avoid Reporting/Record-keeping Requirements

1. 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.
2. Any individual or group that coerces/induces or attempts to coerce/induce a bank employee not to file any reports or any other forms.
3. 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

1. An account of a customer who does not reside/have office near the Business Unit even though there are bank Business Units near his residence/office.
2. A customer who often visits the safe deposit area immediately before making cash deposits, especially deposits just under the threshold level.
3. Funds coming from the list of countries/centers, which are known for money laundering.

Customer who provides Insufficient or Suspicious Information

1. 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.
2. A customer/company who is reluctant to reveal details about its activities or to provide financial statements.
3. A customer who has no record of past or present employment but makes frequent large transactions.

Certain Suspicious Funds Transfer Activities

1. Sending or receiving frequent or large volumes of remittances to /from countries outside India.
2. Receiving large TT/DD remittances from various centers and remitting the consolidated amount to a different account/center on the same day leaving minimum balance in the account.
3. 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

1. An employee whose lavish lifestyle cannot be supported by his or her salary.
2. Negligence of employees/willful blindness is reported repeatedly.

Miscellaneous

Bank no longer knows the true identity
When a bank believes that it would no longer be satisfied that it knows the true identity of the account holder.
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 amount 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 Bankers 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 amount 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 travelers 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 of 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 of
- 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.

Annexure – V

Cross Reference(s)

1. Section 5.3 (ix) Customer Acceptance Policy
2. Section 17.0 - Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967

Government of India

Ministry of Home Affairs CTCR Division

File No.14014/01/2019/CFT March 14 2019

Order

Subject: Procedure for Implementation of Section 51A of the Unlawful (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 51 A, reads as under:-

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

(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;
(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism:
(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism".

The Unlawful Activities (Prevention) Act, 1967 defines "Order" as under:-

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

After the reorganization of the Divisions in Ministry of Home Affairs, the administration of Unlawful Activities (Prevention) Act, 1967 and the work relating to countering of terror financing has been allocated to the CTCR (Counter Terrorism and Counter Radicalization) Division. The order dated 27.8.2009 is accordingly modified as under:

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 CTCR Division would be the Joint Secretary (CTCR), Ministry of Home Affairs. His contact details are 011-23092736 (Tel), 011-23092569 (Fax) and jsctcr-mha@gov.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 CTCR Division in MHA.
iii) The States and UTs should appoint a UAPA Nodal Officer preferably of the rank of the Principal Secretary / Secretary, Home Department and communicate the name and contact details to the CTCR Division in MHA.
iv) The CTCR Division in MHA would maintain the consolidated list of all UAPA Nodal Officers and forward the list to all other UAPA Nodal Officers.
v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA Nodal Officers. to the banks, stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies respectively.
vi) The consolidated list of the UAPA Noda! Officers should be circulated by the Nodal Officer of CTCR Division of MHA in July every year and on every change. Joint Secretary (CTCR) being the Nodal Officer of CTCR Division of MHA, shall cause the amended list of UAPA Noda! Officers to be circulated to the Nodal Officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

Communication of the list of designated individuals / entities

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

i) The Ministry of External Affairs shall update the list of individuals and entities subject to UN sanction measures on a regular basis. On any revision, the Ministry of External Affairs would electronically forward this list to the Nodal Officers in Regulators, FIU-IND, CTCR 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 CTCR 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 (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone or 011-23092736. The particulars apart from being sent by post, should necessarily be conveyed on e-mail id: jsctcr-mha@gov.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 maybe.
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 (CTCR), 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: jsctcr-mha@gov.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 4(ii) above, CTCR 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 by the UAPA Nodal Officer of CTCR Division of MHA 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 CTCR Division of MHA shall also forward a copy thereof to ail 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 CTCR Division of MHA shall also forward a copy of the order to all Directors General of Police / Commissioners of Police of all States / UTs for initiating action under the provisions of the Unlawful Activities (Prevention) Act, 1967.

The order shall be issued without prior notice to the designated individual / entity.

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

7. CTCR 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 (CTCR), 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 jsctcr-mha@gov.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 (CTCR), 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 (CTCR), Ministry of Home Affairs, at Fax No.011-23092569 and also conveyed over telephone on 01123092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail id: jsctcr-mha@gov.in. MHA may also have the verification 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, by the UAPA Nodal Officer of CTCR 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 be issued without prior notice to the designated individual / entity.

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 1967.

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 CTCR Division for freezing of funds or other assets.

15. The UAPA Nodal Officer of CTCR 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 CTCR Division, the procedure as enumerated at paragraphs 4 to 12 above shall be followed.

The freezing orders shall be issued without prior notice to the designated persons involved.

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

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

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

19. The Joint Secretary (CTCR), MHA being the UAPA Nodal Officer for CTCR Division of MHA shall cause such verification, as may be required on the basis of the evidence furnished by the individual / entity, and, if 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 UAPA Nodal Officer of CTCR Division shall inform the applicant.

Communication of Orders under section 51A of Unlawful Activities (Prevention) Act, 1967.

20. All Orders under section 51A of Unlawful Activities (Prevention) Act, 1967 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 Registrars performing the work of registering immovable properties, through the State / UT Nodal Officer by CTCR 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 CTCR 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.

(Piyush Goyal)

Joint Secretary to the Government of India

Annexure- VI

Cross Reference(s) 1. Section 4.11 – Definitions: Beneficial Owner (BO) 2. Section 6.1.5 - Customer Due Diligence: Beneficial Ownership			
The Jammu & Kashmir Bank Limited **Corporate** Headquarters, M A Road, Srinagar, 190001 Kashmir, India	T +91 (0)194 2502689 F+91 (0)194 2502689	E kycaml.chq@jkbmail.com W www.jkbank.net	
KYC AML **Ref:** JKB/CHQ/KYC AML/2017/ August 19th, 2017			

Reg: Identification and incorporation of details of Beneficial Owners of Juridical Person Accounts in Finacle.

Reference is invited to Circular no: 606 dated 11th, December 2013 wherein operative levels were strictly advised to identify the beneficial Owners of all juridical person accounts and incorporate the details of same in Finacle for legacy as well as while opening new accounts. The procedure for incorporating these details was also given in the above referred to circular. The subject guidelines also form part of our latest Reviewed KYC/AML policy, issued vide circular no: 206 dated 26th, July 2016.

2. However, it has been observed that your business unit has given scant attention to these guidelines and has not incorporated these details in such accounts thus exposing the bank to regulatory non-compliance which can have serious repercussions.

3. In order to ensure compliance, a indicative list of such accounts pertaining to your business unit has been extracted centrally where beneficial Owner details are missing. You are advised to go through the list and ensure incorporation of beneficial owner details in CBS in these accounts as per the laid down procedure by or before 15th, September 2017. Pertinent to mention, that the list is not exhaustive. Accordingly, accounts which may have been excluded from the annexed list but fall under the said category should also be included for incorporating beneficial owner details. Similarly, the accounts which figure in the list, however, do not qualify under this category should be excluded from this exercise.

4. For ready reference, these guidelines are reproduced hereunder again for its effective implementation.

5. Definition of "Beneficial Owner":- The term "Beneficial Owner" has been defined as the natural person who ultimately owns or controls a client and /or the person on whose behalf the transaction is being conducted, and includes a person who exercises ultimate effective control over a juridical person. When the Bank identifies a Customer for opening an account, it will identify the beneficial Owner(s) and take all reasonable steps in terms of Rule 9(3) of the PML Rules to verify his identity, as per guidelines provided below:

(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 /have a controlling ownership interest or who exercises control through other means. (Explanation: 1. "Controlling Ownership interest" means ownership of/entitlement to more than 25 percent of the shares or capital or profits of the company 2. "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting

agreements.

(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 /have ownership of/entitlement to more than 15 per cent 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/have ownership of/entitlement to more than 15 percent of the property or capital or profits of the unincorporated association or body of individuals.

(d) Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of Senior Managing Official.

(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 15% or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership.

(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. There exists the possibility that trust/nominee or fiduciary accounts can be used to circumvent the customer identification procedures. In such cases, bank will determine whether the customer is acting on behalf of another person as trustee/nominee or any other intermediary. If so, bank will insist on satisfactory evidence of the identity of the intermediaries and of the persons on whose behalf they are acting, as also obtain details of the nature of the trust or other arrangements in place. The different categories of beneficiaries should be identified as defined above. In the case of a 'foundation', steps should be taken to verify the founder managers/directors and the beneficiaries, if defined.

6. Procedure of incorporation in CBS: After above identification process, the details of beneficial owner/s of the accounts are to be incorporated in CBS as under:-

a) Beneficial Owner must have CUST_ ID, if not then create CUST_ID for beneficial owner/s first.

b) Then modify Cust_ID of the juridical person account (to whom the beneficial Owner/s has to be linked) in CUMM and then populate P-details.

c) In P-details, enter Cust_ ID of the beneficial Owner/s, and then press F11, name of the beneficial Owner will be displayed automatically.

d) In "Reltn" field press F2 and select the code "BFOWN" from the list and press F4-F10 to commit the changes. Then verify in CUMM-V option to reflect the changes.

7. Further, a system check has been put in place in CBS whereby while creating new Cust ID's under "CUMM' in Finacle under customer classification codes specific to juridical person accounts, the system shall prompt the user to punch beneficial owner details.

8. You are directed to ensure that staff members within your business unit who are mainly concerned with this job should take note of these guidelines for its strict compliance. Further, the concerned Users who create/ verify the "CUST ID" with missing beneficial owner details shall be held personally liable.

9. Any non-compliance on this score shall be dealt strictly.