MAYBANK INDONESIA
MUMBAI - INDIA

KYC / AML / CFT

POLICY GUIDELINES & PROCEDURES

March 2022

CONFIDENTIAL

Ver.1.2022

.

DOCUMENT VERSION CONTROL

Version	**:**	**1.2022**
Approval Date	**:**	**MANCO - 29-March-2022**
Last Update	**:**	**June 2021**
Documented By	**:**	**G Viswanathan Head Compliance**
Reviewed By	:	Prasad LV – Head, Treasury Anish Varma – Head Transaction Banking Bharat Pania – Head Corporate Banking Zarina Engineer – Head HR Akshat Bamorya – CRO Meghna – CFO Amrik Singh Gujral – Head Market & Operational Risk Ninad Labre – Head IT
Endorsed By		
Mohit Varma **GM & Country Head**		

LV Prasad	Head – Treasury	
G Viswanathan	Head - Compliance	
Zarina Engineer	Head – HR	
Anish Verma	Head – FI & Transaction Banking	
Bharat Pania	Head – Corporate Banking	
Amrik Singh	Head – Market & Operational Risk	
Akshat Bamorya	CRO	
Meghna	CFO	
Rahul Sanghvi	Head – Operations	
Ninad Labre	Head IT	

CONFIDENTIAL

Table of Contents

1.0	**Introduction**	**….**	**6**
2.0	**Purpose & Scope**	**….**	**6**
3.0	**Customer Acceptance Policy**	**….**	**6**
3.1	**Risk Based Approach to Customer Acceptance**	**….**	**7**
3.2	**Correspondent Relationship with a Banks**	**….**	**9**
3.3	**Prohibited Client Categories**	**….**	**9**
4.0	**Customer Identification Procedures**	**….**	**10**
4.1	**Basic Due Diligence**	**….**	**10**
4.2	**Enhanced Due Diligence (EDD)**	**….**	**11**
4.3	**Beneficial Owner**	**….**	**12**
4.4	**Documentation**	**….**	**13**
4.5	**Officially valid Documents (OVD) & Simplified Measures**	**….**	**15**
4.6	**Small Accounts**	**….**	**16**
4.7	**Unique Customer Identification Code**	**….**	**16**
4.8	**e-KYC Service of UIDAI:**	**….**	**16**
4.9	**Centralised KYC (CKYC)**	**….**	**17**
5.0	**Monitoring Transaction**	**….**	**17**
5.1	**Ongoing Due Diligence**	**….**	**19**
5.2	**Monitoring High Risk Accounts**	**….**	**19**
5.3	**Walk-in customers**	**….**	**19**
6.0	**Risk Management**	**….**	**19**
6.1	**Periodical Review**	**….**	**20**
6.2	**Periodical Updation of customer Identification Data**	**….**	**20**
6.3	**Inoperative Accounts**	**….**	**21**
6.4	**Closure of Accounts**	**….**	**21**

CONFIDENTIAL

7.0 Combating Financing of Terrorism …. 22

7.1 Freezing of Assets under Section 51A of Unlawful Activities .. 23
(Prevention) Act

7.2 Freezing of financial assets …. 24

7.3 Implementation of requests received from foreign countries … 25
under U.N. Security Council Resolution

7.4 Procedure for Unfreezing of funds / Assets …. 25

7.5 Communication of orders …. 26

7.6 Jurisdictions that do not or insufficiently apply the FATF …. 26

8.0 Wire Transfer …. 26

8.1 Cross Border wire transfers …. 27

8.2 Domestic Wire Transfers …. 28

9.0 Principal Officer …. 29

10.0 Maintenance and Preservation of records …. 30

10.1 Maintenance of Records of transactions …. 30

10.2 Preservation of Records …. 30

11.0 Reporting to Financial Intelligence Unit India …. 32

11.1 Cash Transaction Report …. 32

11.2 Suspicious Transaction Report …. 33

11.3 Non Profit Organisation …. 33

11.4 Counterfeit Currency Transaction Report …. 34

11.5 Cross Border Wire Transfer Report …. 34

12.0 Customer Education/Employee's Training/Employee's …. 34
Hiring

12.1 Customer Education …. 34

12.2 Employees Training …. 34

CONFIDENTIAL

12.3 Employees Hiring …. 35

13 Key Accountabilities …. 36

Roles & Responsibilities of other activities …. 36

Annexure 1 – KYC Risk Evaluation Form - Personal …. 37

Annexure II – KYC Risk Evaluation Form Non-Personal …. 42

Annexure III – Customer Identification Procedure Documents …. 49

Annexure IV – Officially Valid Documents (OVD) …. 53

Annexure V – Small Accounts …. 54

Annexure VI - Risk Assessment Table …. 55

CONFIDENTIAL

1. Introduction

This document defines the Bank's policy framework on Know Your Customer (KYC) and Anti Money Laundering (AML) Measures to be put in place, in line with RBI guidelines (Master Direction DBR.AML.BC.No.81/14.01.001/2015-16 dated 25-Feb-2016, updated till 20-April-2020) and OJK Regulation No. 12/POJK.01/2017 dated 21 March 2017 and OJK Circular No. 32/SEOJK.03/2017 dated 22 June 2017 concerning Anti Money Laundering and Counter Financial Terrorism Implementation Program in Financial Service Sector and Law No.9 of 2013 concerning Eradication of Money Laundering.

2. Purpose & Scope

Maybank Indonesia – Mumbai branch adheres to KYC and AML policies in line with RBI guidelines and OJK Regulation concerning Anti Money Laundering and Countering Financial Terrorism. To remain close to the best practice, the bank takes a broad view of the crimes that are related to money laundering, and specifically considers that tax evasion is a money laundering offence.

The purpose of this document is to frame the KYC / AML guidelines based on the following four key elements:

a) Customer Acceptance Policy;
b) Customer Identification Procedures;
c) Monitoring of Transactions; and
d) Risk Management

The scope not only includes the various deposit and loan accounts opened with the bank but also the one-off transactions handled for non-customers like –

- Walk in clients
- Beneficiaries of restricted LCs, who do not have account relationship with us, etc.

3. Customer Acceptance Policy:

There are two steps in the Customer Acceptance process – gathering information as set out in this policy and verifying the information where it is required.

The information to be gathered through an interview with the prospective customer is set out in the appropriate KYC Risk Evaluation Form.

The Risk Assessment and Rating of the customer will be based on the KYC Risk Evaluation Form (Annexure I and II) and as per Risk Assessment Table provided as Annexure VI.

Branch should strictly adhere to the following guidelines before a customer relationship in the bank is started.

CONFIDENTIAL

- 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 organisations etc.

- Circumstances, in which a customer is permitted to act on behalf of another person/entity, should 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.

3.1 Risk Based Approach to Customer Acceptance:

A risk-based approach for the due diligence is to be applied in accepting our customers. In every situation, it must be determined whether the products and services being requested are appropriate to a potential customer. All of our customers must undergo customer due diligence consistent with the risk of the products and services being offered to that customer.

For certain types of customers, additional due diligence must be done to satisfy ourselves that the customer represents an acceptable risk to the Bank.

In other situations, we should not establish a banking relationship with a potential High Risk customer with whom relationship is not advisable.

Bank should prepare a profile for each new customer as per the attached `KYC Risk Evaluation Form' Personal or Non-Personal, as the case may be (Annexure I and II). 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 will depend on the risk perceived by the bank. However, while preparing customer profile bank should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes, without the express permission of the customer.

Where the proposed client cannot be classified under `Prohibited Client Category', the AML Risk rating is to be made by considering the following:

- Individuals (other than High Net Worth) and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile, may be categorised as low risk. Illustrative examples of low risk customers could be salaried employees whose salary structures are well defined, people belonging to lower economic strata of the society whose accounts show small balances and low turnover, Government Departments and Government owned companies, regulators and statutory bodies etc. In such cases,

CONFIDENTIAL

the basic requirements of verifying the identity and location of the customer are to be met.

- Customers who are likely to pose a higher than average risk to the bank should be categorised as medium or high risk depending on customer's background, nature and location of activity, country of origin, sources of funds and his client profile, etc. Bank should apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive ‘due diligence’ for higher risk customers, especially those for whom the sources of funds are not clear.
- If an individual customer does not have any of the Officially Valid Documents (OVDs), as mentioned in Annexure IV below as proof of identity, simplified measures can be applied in respect of low risk customers, as elaborated under para 4.5 below.

In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & jewellers should also be categorized by banks as 'high risk' requiring enhanced due diligence. Other examples of customers requiring higher due diligence include

(a) non-resident customers;

(b) high net worth individuals;

(c) trusts, charities, NGOs and organizations receiving donations;

(d) companies having close family shareholding or beneficial ownership;

(e) firms with 'sleeping partners';

(f) 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;

(g) non-face to face customers,

(h) bullion dealers & jewellers, etc.

In addition to what has been indicated above, bank should take steps to identify and assess their ML/TF risk for customers, countries and geographical areas as also for products/ services/ transactions/delivery channels.

Accounts of non-face-to-face customers

a) In the case of non-face-to-face customers, apart from applying the usual customer identification procedures, branch need to have adequate procedures to mitigate the higher risk involved.

b) Certification of all the documents presented should be insisted

c) if necessary, additional documents may be called for

d) branch may ask the first payment to be effected through the customer's account with another bank which, in turn, adheres to similar KYC standards

CONFIDENTIAL

e) In the case of cross-border customers, certification should be from Embassy or Maybank Group branches, or Correspondent Banks where we have SWIFT RMA. Overseas Correspondent Bank should be requested to confirm KYC by SWIFT.

3.2 Correspondent relationship with Banks:

Bank should be extremely cautious while continuing relationships with correspondent banks located in countries with poor KYC standards and countries identified as 'non-cooperative' in the fight against money laundering and terrorist financing. Banks should ensure that their respondent banks have anti money laundering policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts.

3.3 Prohibited Client Categories:

Maybank, Mumbai will strictly reject any new client accounts for the following client categories:

- Anonymous or fictitious / benami name;
- Massage Parlours / Escort Services / Adult content websites
- Money / Currency Exchange Houses
- Factoring Companies / Direct Sales & Marketing companies
- Pyramid Sales Schemes / Internet Gaming / Virtual Casinos
- Sales & Distribution of Pornographic material and other sexual communication
- Potential client or entity name is enlisted in negative news list, e.g. OFAC List, Terrorist List, Terrorist and Organisational Terrorist List or within Internal Bank watch list.
- Potential customer is enlisted in any of the Caution Lists circulated by Reserve Bank of India.
- Shell Banks or a part of shell bank or has correspondent relationship with a shell bank.
- Potential customer is found to have submitted fake information to the bank.
- Prohibit new account and close existing account where the bank is unable to apply appropriate customer due diligence measures, i.e. bank is unable to verify the identity and/or obtain documents required as per the risk categorisation due to non-co-operation of the customer or non-reliability of the data/information furnished to the bank.
- Suspicions that customer own funds or asses regulated/controlled by terrorist, or used to fund act of terrorism could be confirmed.

- Not to open an account or close an existing account where the bank is unable to apply appropriate customer due diligence measures, i.e., bank is unable to verify the identity and /or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-

CONFIDENTIAL

reliability of the data/information furnished to the bank. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer.

- Decision by the bank to close an account should be taken at a reasonably high level (Head of Operations / Head of Global Banking) after giving due notice of two weeks from the date of the notice to the customer explaining the reasons for such a decision.

4. Customer Identification Procedures:

Relationship Managers are primarily responsible for and must ensure that client information is kept upto date at all times.

Customer Identification Procedure is carried out at different stages, mainly –

(a) during inception, i.e. while establishing a banking relationship;
(b) When carrying out a financial transaction; or
(c) When the bank has a doubt about the authenticity/veracity or the adequacy of the previously obtained customer identification data

Customer identification means identifying the customer and verifying his/her identity by using reliable, independent source documents, data or information. Bank need to obtain sufficient information necessary to establish, to their satisfaction, the identity of each new customer, whether regular or occasional, and the purpose of the intended nature of banking relationship. Being satisfied means that the bank must be able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the extant guidelines in place.

4.1 Basic Due Diligence:

The Basic Due Diligence requirements for establishing and maintaining client relationship with the Bank requires obtaining and verifying the following:

• Client's identity, including any aliases;
• Client's residential address;
• Appropriate verification of client's identity and residential address;
• Documentation of the money laundering/terrorist financing risks assessment associated with the customer;
• Obtaining information on the purpose and intended nature of the business relationship with the Bank;
• For non-personal account clients, determining the beneficial owner(s) of any non-individual account and verifying their identity;
• Anticipated account activity; Customer information need to be collected for expected transaction activity in the account.
• Nature and details of client's business or the business of the entity opening the account;

CONFIDENTIAL

• Source of Wealth: Source of funds of the client
• Confirming that all the account(s) will not be used for activity by or on behalf of anyone other than the named account holder(s) ("Third Party Determination");
• Checking new customer names and beneficial owners, against prescribed Government sanctions lists and lists of Politically Exposed Foreign Persons.
• Relevant US FATCA - CRS tax form most appropriate for the client or Party. In the case of individuals the Bank can assume that the Client and the Beneficial Owner are one and the same. If there are any doubts as to whether the Client and the Beneficial Owner are one and the same person, or if it is obvious that the Client is a different person than the Beneficial Owner, Beneficial Ownership must be confirmed and Minimum CDD Requirements must be applied to both Client and Beneficial Owner.

4.2 Enhanced Due Diligence (EDD):

Higher Risk Customers must undergo EDD in addition to Basic Customer Due Diligence.

We conduct Enhanced Due Diligence on Higher Risk customers because these are customers who have an inherently higher risk of money laundering. However, there are many customers who may pose a higher risk that the Bank would be willing to do business with, once it has satisfied itself through EDD that the customer is legitimate and the expected activity is reasonable given what we know about the customer and its industry.

EDD is intended to:

- Provide an enhanced analysis of the money laundering/terrorist financing risk and legitimacy of the proposed customer, based on the history of the customer, the types of products and services offered to the customer, source of funds, purpose of transactions, review of counter-parties, countries where the customer will be conducting business, and the appropriateness of the banking products requested given what we have learned about that customer;

- Complete additional verification to confirm that the information collected through basic Customer Due Diligence is completed and accurate;

- Obtain an Opinion letter from the existing bankers as to their dealings

- Determine whether the Bank should accept this customer, despite being considered as Higher Risk; and

CONFIDENTIAL

- Establish through the KYC Risk Evaluation Form, the expected activity for the customer's accounts. This will be the basis of future monitoring of actual activity through the accounts.

Restricted Customers are customers for whom the Bank will not open accounts and will exit an existing relationship, if it finds that the customer should be classified as a Restricted Customer. This is because the Customer appears to be involved in activity that may be illegal or poses potential reputational risk to the Bank, or the Bank cannot otherwise confirm that the customer is legitimate. The detailed lists of restricted customers and High Risk customers are available in the KYC Risk Evaluation Form – Non Personal (Annexure II)

There are two steps in the Customer Acceptance process – gathering information as set out in this policy and verifying the information, where it is required.

The information to be gathered through an interview with the prospective customer is set out in the appropriate **KYC Risk Evaluation Form.**

The Risk Assessment and Rating of the customer will be based on the KYC Risk Evaluation Form (Annexure I and II) and as per the Risk Assessment Table provided as Annexure VI.

All High Risk accounts need to be reviewed and approved by Head of Global Banking / Head of Compliance before opening the account.

4.3 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. Government of India has since examined the issue and has specified the procedure for determination of Beneficial Ownership. The procedure as advised by the Government of India is as under:

A. Where the client is a person other than an individual or trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the following information:

(i) The identity of the natural person, who, whether acting alone or together, or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest.

Explanation: Controlling ownership interest means ownership of/entitlement to more than 25 percent of shares or capital or profits of the juridical person, where the juridical person is a company; ownership of/entitlement to more than 15% of the capital or profits of the juridical person where the juridical person is a partnership; or, ownership

CONFIDENTIAL

of/entitlement to more than 15% of the property or capital or profits of the juridical person where the juridical person is an unincorporated association or body of individuals.

(ii) In cases where there exists doubt under (i) as to whether the person with the controlling ownership interest is the beneficial owner or where no natural person exerts control through ownership interests, the identity of the natural person exercising control over the juridical person through other means.

Explanation: Control through other means can be exercised through voting rights, agreement, arrangements, etc.

(iii) Where no natural person is identified under (i) or (ii) above, the identity of the relevant natural person who holds the position of senior managing official.

B. Where the client is a trust, the banking company and financial institution, as the case may be, shall identify the beneficial owners of the client and take reasonable measures to verify the identity of such persons, through the identity of the settler of the trust, the trustee, the protector, 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.

C. 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.

D. Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a majority-owned subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

4.4 Documentation:

For customers who are natural persons, the bank should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph.

For customers who are legal persons or entities, the bank should

i. verify the legal status of the legal person/entity through proper and relevant documents;

ii. verify that any person purporting to act on behalf of the legal person/entity is so authorised and identify and verify the identity of that person;

CONFIDENTIAL

CONFIDENTIA

(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.

(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 Customer Due Diligence (CDD) procedure is to be completed. If the CDD procedure 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.

(vi) 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 either with us or with any other Bank. Further, while uploading KYC information to CKYCR, 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.

(vii) Banks shall have strict monitoring procedures including systems to generate alerts in case of any non-compliance/violation, to ensure compliance with the above mentioned conditions.

4.9 Centralised KYC (CKYC):

Bank should upload the KYC data pertaining to all individual accounts with CERSAI in terms of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005.

The Government of India has authorised the Central Registry of Securitisation Asset Reconstruction and Security Interest of India (CERSAI) to act as and to perform the functions of the Central KYC Records Registry under the said rules, including receiving, storing, safeguarding and retrieving the KYC records in digital form of a “client”.

Head – Compliance will be the Nodal Officer and Head – Operations & IT and Head of Branch Operations will be the Admin Users.

5. Monitoring of Transactions

CONFIDENTIAL

Ongoing monitoring is an essential element of effective KYC procedures. We can effectively control and reduce their 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. Banks should pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

Bank should monitor the turnover in the accounts vis-à-vis the expected activity declared in the account opening form / KYC Risk Evaluation Form. Transactions that involve large amounts of cash inconsistent with the normal and expected activity of the customer should particularly attract the attention of the bank. Very high account turnover inconsistent with the size of the balance maintained may indicate that funds are being 'washed' through the account.

Transaction monitoring guidelines, including transactions from and to High Risk Country:

`Worldcheck or equivalent screening system' and `AML Compass System' are primarily considered the `Core Systems' supporting KYC AML function for monitoring transactions.

- Before opening of accounts, the names of all beneficial owners are scanned through WorldCheck and it is ensured that no positive match is found.
- All transactions of INR 100,000 and above, in all the accounts, will be monitored by Head-Branch Ops and the Relationship Manager on a continuous basis.
- Any suspicious activity, including any unusual transaction or structuring of transactions noticed will be escalated to Head – Global Banking, Operation & Technology and Compliance for further review and actions, if any.
- All cash transactions aggregating INR 1 Million and above in any account during a calendar month needs to be reported to FIU, India on a monthly basis.
- All outward remittances and Letter of Credits opened will be scanned through WorldCheck for any possible match for beneficiary or the country and any positive match will be escalated to Head – Global Banking, Operation & Technology and Compliance for further review and actions, if any
- Scanning all Outward remittances and all Letter of Credits through WorldCheck helps to monitor all cross country transactions closely and take necessary steps.

All transactions conducted during the day will be analysed by the AML Compass System after the day end and will generate alerts based on the various scenarios and thresholds set as per IBA guidelines. All these alerts will be monitored by

CONFIDENTIAL

Head of Branch Operations, and Head of Trade Operations as reviewers and Head Operations and Head Compliance will be reviewing and approving them on a daily basis.

All alerts generated should be reviewed / approved within two working days. An update on the status of AML/Sanction screening alerts pending for closure should be placed before MANCO on a monthly basis.

5.1 Ongoing Due Diligence

Bank should 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 their knowledge of the client, his business and risk profile and where necessary, the source of funds [Ref: Government of India Notification dated June 16, 2010 –Rule 9, sub-rule (1B)]

5.2 Monitoring of High Risk Accounts

High-risk accounts have to be subjected to intensified monitoring. Bank should set key indicators for such accounts, taking note of the background of the customer, such as the country of origin, sources of funds, the type of transactions involved and other risk factors. High risk associated with accounts of bullion dealers (including sub-dealers) & 19jewellers19 should be taken into account by banks to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to Financial Intelligence Unit- India (FIU-IND)

5.3 Walk-in customers

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

As per Prevention of Money Laundering Rules, 2005 banks and financial institutions are required to verify the identity of the customers for all international money transfer operations.

6. Risk Management

KYC programme as enumerated in the policy should be put in place and followed scrupulously to ensure its effective implementation.

CONFIDENTIAL

- Risk profiles for all customers should be invariably created by filling in the appropriate KYC Risk Evaluation Form.
- WorldCheck review need to be performed on the proposed customer, beneficiary of LC /Remittance, etc. and ensure there is no positive match before opening the account / undertaking the transaction.
- All High Risk accounts need to be reviewed and approved by Head of Global Banking and Head of Compliance before opening the account.
- All new accounts and transactions will be subject to compliance review.
- Staff should be imparted relevant training at regular intervals to keep themselves updated.

6.1 Periodical Review

A periodical review of risk categorization of accounts is to be carried out and enhanced due diligence measures need to be applied wherever required. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months. This should be carried out by the concerned RM and Head - Branch Ops.

The review should cover the general activity in the account, volume of turnover vis-à-vis the anticipated turnover declared at the time of opening the account, any suspicious activity noted during the period, etc.

Any material / significant issues / finding arising from the review will be escalated to HO Internal Audit function.

6.2 Periodical Updation of Customer Identification Data

(a) Periodic updation shall be carried out at least annually for high risk customers, once in every three years for medium risk customers and once in every five years for low risk customers as per the following procedure:

i) PAN verification from the verification facility available with the issuing authority 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 categorised 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.

CONFIDENTIAL

v) In case of Legal entities, Bank shall review the documents sought at the time of opening of account and obtain fresh certified copies.

(b) Bank 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] Bank 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.

(e) Fresh photographs shall be obtained from customer for whom account was opened when they were minor, on their becoming a major.

6.3 Inoperative accounts

Savings as well as current accounts should be treated as inoperative/dormant if there are no debit or credit transactions induced at the instance of customer in the account for over a period of two years. RBI has clarified that dividends on shares credited to the accounts as per mandate given by the customers has to be treated as customer induced transactions.

Branch should make an annual review of accounts in which there are no operations (i.e., no credit or debit other than crediting of periodic interest or debiting of service charges) for more than one year. They may approach the customers and inform them in writing that there has been no operation in their accounts and ascertain the reasons for the same. In case the non- operation in the account is due to shifting of the customers from the locality, they may be asked to provide the details of the new bank accounts to which the balance in the existing account could be transferred.

To avoid misuse and fraud in in-operative accounts, the operations in the account should be allowed only after ensuring genuineness of the transaction, verification of the signature and identity etc. All transactions to be authorised by the Head of Operations.

6.4 Closure of accounts

Where the bank is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the bank should consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for

CONFIDENTIAL

taking such a decision. Such decisions need to be taken at a reasonably senior level, by Head of Global Banking and Head of Operations.

7. Combating Financing of Terrorism

a)In terms of PMLA Rules, suspicious transaction should include, inter alia, transactions, which give rise to a reasonable ground of suspicion that these may involve financing of the activities relating to terrorism. Banks are, therefore, advised to develop suitable mechanism through appropriate policy framework for enhanced monitoring of accounts suspected of having terrorist links and swift identification of the transactions and making suitable reports to FIU-India on priority.

b) As and when list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), are received from Government of India, Reserve Bank circulates these to all banks and financial institutions. Banks/Financial Institutions should ensure to update the lists of individuals and entities as circulated by Reserve Bank. The UN Security Council has adopted Resolutions 1988 (2011) and 1989 (2011) which have resulted in splitting of the 1267 Committee's Consolidated List into two separate lists, namely:

- "Al-Qaida Sanctions List", which is maintained by the 1267 / 1989 Committee. This list shall include only the names of those individuals, groups, undertakings and entities associated with Al-Qaida. The Updated Al-Qaida Sanctions List is available at
- http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml

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

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

Before opening any new account it should be ensured that the name/s of the proposed customer does not appear in the lists. Further, banks should scan all existing accounts to ensure that no account is held by or linked to any of the entities or individuals included in the list.

`WorldCheck' includes all the above lists and hence checking through WorldCheck is sufficient for our Bank.

CONFIDENTIAL

AML System screens the database on a daily basis with updated lists and all existing accounts are checked. Full details of accounts bearing resemblance with any of the individuals / entities in the list should immediately be intimated to RBI and FIU-IND.

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

i)The Unlawful Activities (Prevention) Act, 1967 (UAPA) has been amended by the Unlawful Activities (Prevention) Amendment Act, 2008. Government has issued an Order dated August 27, 2009 detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 relating to the purposes of prevention of, and for coping with terrorist activities. In terms of Section 51A, the Central Government is empowered to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism and prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.

ii) Banks are required to strictly follow the procedure laid down in the UAPA Order dated August 27, 2009 and ensure meticulous compliance to the Order issued by the Government.

iii) On receipt of the list of individuals and entities subject to UN sanctions (referred to as designated lists) from RBI, banks should 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 their customers match with the particulars of designated individuals/entities, the banks 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) Banks 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, Central Office, Reserve Bank of India, Anti Money Laundering Division, Central Office Building, 13th Floor, Shahid Bhagat Singh Marg, Fort, Mumbai – 400 001 and also by fax at No.022-22701239. The particulars apart from being sent by post/fax should necessarily be conveyed on e-mail.

d) Banks 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 banks would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

f) Banks 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.

7.2 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 banks are the ones listed as designated individuals/entities and the funds, financial assets or economic resources or related services , reported by banks 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

CONFIDENTIAL

the concerned bank branch under intimation to Reserve Bank of India and FIU-IND.

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

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

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

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

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

d) Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to banks and the procedure as enumerated above shall be followed.

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

7.4 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:

CONFIDENTIAL

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.

7.5 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.

7.6 Jurisdictions that do not or insufficiently apply the FATF

Recommendations of RBI

a) Banks are required to take into account risks arising from the deficiencies in AML/CFT regime of the jurisdictions included in the FATF Statement. In addition to FATF Statements circulated by Reserve Bank of India from time to time, banks should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that banks should also give special attention 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.

b) Banks should 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 should, as far as possible be examined, and written findings together with all documents should be

CONFIDENTIAL

retained and made available to Reserve Bank/other relevant authorities, on request.

8. Wire Transfer

Banks use 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.

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.

Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, there is a need for preventing terrorists and other criminals from having unfettered access to wire transfers for moving their funds and for detecting any misuse when it occurs. This can be achieved if basic information on the originator of wire transfers is immediately available to appropriate law enforcement and/or prosecutorial authorities in order to assist them in detecting, investigating, prosecuting terrorists or other criminals and tracing their assets. The information can be used by Financial Intelligence Unit – India (FIU-IND) for analysing suspicious or unusual activity and disseminating it as necessary. The originator information can also be put to use by the beneficiary bank to facilitate identification and reporting of suspicious transactions to FIU-IND. Owing to the potential terrorist financing threat posed by small wire transfers, the objective is to be in a position to trace all wire transfers with minimum threshold limits. Accordingly, banks must ensure that all wire transfers are accompanied by the following information:

CONFIDENTIAL

8.1 Cross-border wire transfers:

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

b) 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.

c) 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 per (b) above.

8.2 Domestic wire transfers:

i. Information accompanying all domestic wire transfers of Rs.50000/- (Rupees Fifty Thousand) and above must include complete originator information i.e. name, address and account number etc., unless full originator information can be made available to the beneficiary bank by other means.

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

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

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

(iv) Role of Ordering, Intermediary and Beneficiary banks

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

CONFIDENTIAL

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

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

9. Principal Officer

a) Banks should appoint a senior management officer to be designated as Principal Officer. Banks should ensure that the Principal Officer is able to act independently and report directly to the senior management or to the Board of Directors. Principal Officer shall be located at the head/corporate office of the bank and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. He 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.

b) Further, the role and responsibilities of the Principal Officer should 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 from time to time. The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organisations of value more than Indian Rupees One Million or its equivalent in foreign currency to FIU-IND.

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

CONFIDENTIAL

d) **The Head of Compliance will be the Principal Officer of the Bank to undertake these responsibilities.**

10. Maintenance of Records of transactions/Information to be preserved/ Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND):

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of Section 12 of the Act ibid.

10.1 Maintenance of records of transactions

Banks should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of PML Rules, 2005, as mentioned below:

a) all cash transactions of the value of more than INR One Million or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been valued below INR One Million 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 INR One Million;

c) all transactions involving receipts by non-profit organisations of value more than INR One Million or its equivalent in foreign currency [Ref: Government of India Notification dated November 12, 2009- Rule 3,sub-rule (1) clause (BA) of PML Rules]

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 a document has taken place facilitating the transaction and

e) All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

10.2 Preservation of Records

Banks should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be

CONFIDENTIAL

retrieved easily and quickly whenever required or when requested by the competent authorities.

(i) In terms of PML Amendment Act 2012, banks/FIs should maintain for at least five years from the date of transaction between the bank/FI 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.

(ii) Banks/FIs should ensure that records pertaining to the identification of the customers and their 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 Seven years after the business relationship is ended. The identification of records and transaction data should be made available to the competent authorities upon request.

(iii)Banks/FIs may maintain records of the identity of their clients, and records in respect of transactions referred to in Rule 3 in hard or soft format.

(iv)As mentioned in paragraph 3.3.1 (b) (i) of this Master Circular, banks/FIs are required to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors to scrutinize the transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for Seven years.

a) Banks are required to maintain the records containing information of all transactions including the records of transactions detailed in Rule 3 above. Banks should take appropriate steps to evolve a system for proper maintenance and preservation of account information in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. Further, banks should maintain for at least ten years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

b) Banks should ensure that 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 Seven years after the business relationship is ended The identification records and transaction data should be made available to the competent authorities upon request.

c) In paragraph 3.3.1 (b) (i) of this Master Circular, banks have been advised to pay special attention to all complex, unusual large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. It is further clarified that the background including all documents/office records/memorandums pertaining to such transactions and purpose thereof should, as far as possible, be examined and the findings at branch as well as Principal Officer level should be properly recorded. Such records and related documents should be made available to help auditors in their day-to-day work relating to scrutiny of transactions and also to Reserve Bank/other relevant authorities. These records are required to be preserved for ten years as is required under PMLA, 2002.

11 Reporting to Financial Intelligence Unit – India

In terms of the PMLA Rules, banks are required to report information relating to cash and suspicious transactions and all transactions involving receipts by non-profit organisations of value more than INR One Million or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi -110021
Website – http://fiuindia.gov.in/

11.1 Cash Transaction Report (CTR)

Bank should scrupulously adhere to the following:

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

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

CONFIDENTIAL

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

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

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

11.2 Suspicious Transaction Reports (STR)

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

ii. It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. It is clarified that banks should report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

iii. Banks should make STRs if they have 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) should 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 should record his reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion once a suspicious transaction report is received from a branch or any other office. Such report should be made available to the competent authorities on request.

v. Banks should not put any restrictions on operations in the accounts where an STR has been made. Banks and their employees should keep the fact of furnishing of STR strictly confidential, as required under PML Rules. It should be ensured that there is no tipping off to the customer at any level.

11.3 Non-Profit Organisation

The report of all transactions involving receipts by non- profit organizations of value more than INR One Million or its equivalent in foreign currency should be

CONFIDENTIAL

submitted every month to the Director, FIU-IND by 15th of the succeeding month in the prescribed format.

Non-Profit Organisation (NPO) means any entity or organisation that is registered as a Trust or a Society under the Societies Registration Act, 1860or any similar State Legislation or a company registered under Section 8 of the Companies Act, 2013.

11.4 Counterfeit Currency Transaction Report

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 a document has taken place facilitating the transaction should be filed with FIU-IND by 15th of the succeeding month.

11.5 Cross-border Wire Transfer

Cross-border Wire Transfer Report (CWTR) is required to be filed with FIU-IND 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, where either the origin or destination of funds is India.

12. Customer Education/Employee's Training/Employee's Hiring

12.1 Customer Education

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

12.2 Employees' Training

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

Employees will be trained internally and would also be deputed for trainings conducted by RBI / FEDAI, etc. There will be refresher trainings at regular intervals, atleast once in a quarter, through KYC/AML/Fraud Monitoring Committee meetings, where all recent changes and live cases will be discussed.

CONFIDENTIAL

HR should keep a record of all KYC/AML/CFT training delivered to their employees.

CONFIDENTIAL

12.3 Hiring of Employees

It may be appreciated that KYC norms/AML standards/CFT measures have been prescribed to ensure that criminals are not allowed to misuse the banking channels. It would, therefore, be necessary that adequate screening mechanism is put in place by banks as an integral part of their recruitment/hiring process of personnel.

CONFIDENTIAL

13. Key Accountabilities:

Minimum CDD Requirement/EDD - Verification and Identification of Customers							
No	Stage/ Roles	On Boarding		Maintenance *(profile change usually triggered by Customer such as change of company name/address/business profile, etc or by transactional activities)*		Periodic Review	
		Minimum Requirement	EDD Requirement	Minimum Requirement	EDD Requirement	Minimum Requirement	KYC updation
1	Head – Branch Operations – (for Individual customers only)	Conduct an interview with prospective customer and fill in the Risk profile.	Where customer is PEP or coming under any of the High Risk category, do EDD and get it approved by Head – Global Banking / Head of Compliance.	Revisit customer to obtain documents that proves change of customer information	EDD where applicable	Conduct a review of the activity in the account, to decide whether any change in the risk gradation.	Full KYC and updation of documents once in 5 years for Low Risk and once in 3 years for Medium Risk and annually for High Risk
2	Relationship Manager (For non-individual accounts)	Conduct an interview with prospective customer and fill in the Risk profile.	Where customer is coming under any of the High Risk category, do EDD and get it approved by Head – Global Banking / Head of Compliance.	Revisit customer to obtain documents that proves change of customer information	EDD where applicable	Conduct a review of the activity in the account, to decide whether any change in the risk gradation.	Full KYC and updation of documents once in 5 years for Low Risk and once in 3 years for Medium Risk and annually for High Risk
3	Head – Global Banking / Head - Compliance	Overall review of Medium and High Risk accounts	Any additional EDD wherever needed and review of positive hits in World Check.	Overall review & approval of Medium and High Risk accounts		Overall review & approval of Medium & High Risk accounts	

Roles & Responsibilities of other activities:

	Responsibility	Roles	Periodicity
1.	Due Diligence of Cross Border Transactions (Letter of Credits, Guarantees, Remittances, etc.), including scanning of beneficiary name / vessel name, etc.	Head – Trade Operations and Head – Operations & IT	While handling such transactions
2.	Review and monitoring of daily transactions	Head – Branch Operations Head – Trade Operations Head – Operations & IT Head – Compliance	Review of various alerts thrown by the AML System on a daily basis and action as required.
3.	Prepare & submit following reports to Financial Intelligence Unit, India Cash Transaction Report Non-Profit Organisation Transaction Report Suspicious Transaction Report Counterfeit Currency Transaction Report Cross Border Wire Transfer Report	Head – Branch Operations Head – Trade Operations Head – Operations & IT Head – Compliance Compass AML System will provide the relevant reports at the relevant periodic intervals. The reports are to be submitted to FIU – India online by Head – Compliance or Head – Operations & IT.	All reports are monthly except Suspicious Transactions Report which is to be sent within seven days of arriving at a conclusion

CONFIDENTIAL

Annexure I

Know Your Customer Risk Evaluation Form (PERSONAL)

Name of Customer :

Brief Introduction. (While interviewing a potential customer, take the time to understand the structure, purpose and identity of the business/individual. Use checklist below to assist in gathering information in an endeavour to know your customer. Document all responses.)

Identify individual customer's needs..

Discuss how our Products and Services will best suit their needs

Is the customer a Politically Exposed Person (PEP) ? or a relative of a PEP ?

(Such customers require EDD and to be classified as High Risk Account)

What type of Business/employment is the customer involved in? Employer details and phone number.

CONFIDENTIAL

Purpose and Reason for Opening the account or establishing the relationship:
Anticipated Level of activity in first year of operations:
Can the customer's source of funds be established? □ Where will the money come from? □ How will it arrive? □ Annual income
How was the wealth acquired? □ How does potential customer maintain wealth? □ How is new wealth acquired?

CONFIDENTIAL

How will potential customer conduct transactions?

☐ Wire transfer. ☐ Cheques. ☐ Cash ☐ TC. ☐ Money order

☐ Foreign Drafts. ☐ Direct deposit by third party

☐ *What will be the frequency and amounts?*

Does this customer plan to move value from one jurisdiction to another in what could be conceived as an opportunity to conceal the source of funds?

Corroborate, Verify and Document what is known.

☐ Business and Personal references (Bank and quantifiable sources).

CONFIDENTIAL

Verification.

- ☐ Permanent Address Validated. (Introduction letter sent at local address/Personal visit done by _____Initials_____.
- ☐ Telephone number validated? Validate landlines and cellular. Office number and residence. (Copy of telephone directory) Done by _____ Initial _____.
- ☐ Employer contacted and details of customer verified. Done by _____ Initials

Categorization of accounts:

☐ Low ☐ Medium ☐ High risk

Individual's identities are established and relevant identification documents have been verified. We are also satisfied about the purpose of the intended nature of banking relationship and the account may be opened.

The Risk categorisation is as above.

Name :

Signature :

(RM)

Name :

Signature:

(Branch Ops)

CONFIDENTIAL

(Place to note your observations, if any)

CONFIDENTIAL

Annexure II

Know Your Customer Risk Evaluation Form
(NON-PERSONAL)

Name of Customer :

Brief Introduction. (While interviewing a potential customer, take the time to understand the structure, purpose and identity of the business/individual. Use checklist below to assist in gathering information in an endeavor to know your customer. Document all responses.)

The market capitalization data :

	52 week range	Market capitalization	No. of shares

The Company's website is :

Type of Business:

Purpose and Reason for Opening the account or establishing the relationship:

Identify products, major suppliers and their geographic locations.

CONFIDENTIAL

Is the Company carrying on Restricted Business: *□ Yes □ No.*

*(*Those individuals/business with which the Bank simply does not entertain requests for business relationships. Can be described as businesses that engage in illegal, quasi-legal, or inappropriate services that expose the Bank to legal, regulatory or reputational risk. Care and diligence are required in dealing with existing customers engaged in Restricted Businesses.)

- Massage Parlours * Escort Services * Adult Content Web Sites * Factoring Co
- Telegraph / Wire Tfr * Money / Currency Exchange Houses * Telephone Card Sales
- Pyramid Sales Schemes * Fantasy Phone Call Companies * Internet Gaming
- Internet or Virtual Casinos * Direst Sales / Marketing * Cam bios
- Sale / Distribution of Pornographic, or obsolete material, and other sexual communications.

If Yes, the request should be avoided and need not be entertained.

Is the Company carrying on High Risk Business: *□ Yes □ No.*

(Those individuals/businesses that present a higher risk of involvement in illegal activity, and with whom the Bank may do business, but only with the prior approval of the Head – Global Banking and Head – Compliance)

If "Yes" prior approval of Manger- AML/Compliance at Supervising Office approval obtained. □ Yes □ No

An indicative list of High Risk Customers:

(a) non-resident customers;

(b) high net worth individuals;

(c) trusts, charities, NGOs and organizations receiving donations;

(d) companies having close family shareholding or beneficial ownership;

(e) firms with 'sleeping partners';

(f) 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;

(g) non-face to face customers,

(h) bullion dealers & jewellers, etc.

CONFIDENTIAL

Identify individuals (i.e. the beneficial owners and authorised officers of the accounts)
***Review registered documents of the company to ensure conformance with local legal registration requirement within the jurisdiction*.**
***Describe the business operations*.**
Describe how product(s) is/are produced or services rendered.

CONFIDENTIAL

***Describe how the product is/ are distributed/service is provided*.**
***Discuss Customer business locations, operation sites and headquarters*.**
Have customer provided the latest Financial Statements?
Can the customer's source of funds be established?
Expected turnover and anticipated volume in the account ?

CONFIDENTIAL

How will potential customer conduct transactions?

☐ Wire transfer. ☐ Cheques. ☐ Cash ☐ TC. ☐ Money order

☐ Foreign Drafts. ☐ Direct deposit by third party

☐ *What will be the frequency and amounts?*

Does this customer plan to move value from one jurisdiction to another in what could be conceived as an opportunity to conceal the source of funds?

Does this customer have reasons to readily convert cash to monetary instruments?

Does the product and services that are being asked for make sense given the nature of the account or business?

Corroborate, Verify and Document what is known.

☐ Visits

☐ Periodicals, Product Brochures, Business and Marketing Literature.

☐ Business and Personal references (Bank and quantifiable sources).

☐ Copy of Annual report.

CONFIDENTIAL

Verification.

☐ Permanent Address Validated? Done by _____ Initials_____.

☐ Telephone number validated? Done by _____ Initials _____.

Categorization of accounts as per RBI requirements.

☐ Low ☐ Medium ☐ High risk

Relevant due diligence to determine the Firm / Company's identity, nature of business, source of wealth / income, expected turnover / volume, etc. have been carried out and relevant identification documents have been verified. We are also satisfied about the purpose of the intended nature of banking relationship and the account may be opened.

The Risk categorization is as above.

Name :

Signature :

(RM)

Name :

Signature:

(Branch Ops)

CONFIDENTIAL

(Place to note your observations)

CONFIDENTIAL

Annexure - III

Customer Identification Procedure

Features to be verified and documents that may be obtained from customers Features	Documents
Accounts of individuals - Proof of Identity and address	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving License (v) Job Card issued by NREGA duly signed by an officer of the State Govt (vi) The letter issued by the Unique Identification Authority of India (UIDAI) containing details of name, address and Aadhaar number Where 'simplified measures' are applied for verifying the identity of customers the following documents shall be deemed to be 'officially valid documents: i) identity card with applicant's Photograph issued by Central/State Government Departments, Statutory/Regulatory Authorities, Public Sector Undertakings, Scheduled Commercial Banks, and Public Financial Institutions; ii) letter issued by a gazetted officer, with a duly attested photograph of the person. Where 'simplified measures' are applied for verifying for the limited purpose of proof of address the following additional documents are deemed to be OVDs :. 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

CONFIDENTIAL

	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
Accounts of companies - Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number	(i) Certificate of incorporation (ii)Memorandum & Articles of Association (iii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iv) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (v) Copy of PAN An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf.
Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Registration certificate (ii) Partnership deed (iii) An officially valid document in respect of the person holding an attorney to transact on its behalf.

CONFIDENTIAL

Accounts of trusts - Names of trustees, settlors, beneficiaries and signatories	(i) Certificate of registration (ii) Trust Deed (iii) Power of Attorney granted to transact business on its behalf (iv) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power of Attorney, founders/ managers/ directors and their addresses
Accounts of Proprietorship Concerns Proof of the name, address and activity of the concern	Apart from Customer identification procedure as applicable to the proprietor any two of the following documents in the name of the proprietary concern would suffice: • Registration certificate (in the case of a registered concern) • Certificate/licence issued by the Municipal authorities under Shop & Establishment Act, • Sales and income tax returns •CST/VAT/GST certificate (Provisional /final) • Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. . Importer Exporter Code (IEC) issued to the proprietary concern by the office of DGFT / License / Certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. • Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. The 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. In cases where the banks are satisfied that it is not possible to furnish two

CONFIDENTIAL

	such documents, they would have the discretion to accept only one of those documents as activity proof. In such cases, the banks, however, would have to undertake contact point verification, collect such information as would be required to establish the existence of such firm, confirm, clarify and satisfy themselves that the business activity has been verified from the address of the proprietary concern.
Accounts of Unincorporated association or a body of individuals	(a) resolution of the managing body of such association or body of individuals (Body of Individuals includes Societies); (b) power of attorney granted to him to transact on its behalf; (c) an officially valid document in respect of the person holding an attorney to transact on its behalf; and (d) such information as may be required by the bank to collectively establish the legal existence of such an association or body of individuals. Explanation: Unregistered trusts/ partnership firms shall be included under the term 'unincorporated association'. Explanation: Term 'body of individuals' includes societies.
Accounts of Juridical persons such as Government or its Departments, Societies, Universities and Local bodies like Village Panchayats	A certified copy of the following documents shall be obtained: 1. Document showing the name of the person authorised to act on behalf of the entity 2. OVD for proof of identity and address in respect of the person holding a power of attorney to transact on its behalf and 3. Such documents as may be required to establish the legal existence of such an entity / judicial person.

CONFIDENTIAL

Annexure IV

"Officially valid document" (OVD)

Officially Valid Document (OVD) means –

- the passport,
- the driving licence,
- the Permanent Account Number (PAN) Card,
- the Voter's Identity Card issued by the Election Commission of India,
- job card issued by NREGA duly signed by an officer of the State Government,
- letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number, or
- any other document as notified by the Central Government in consultation with the Regulator.

Simplified Measures: The following documents shall be deemed to be OVD where simplified measured are applied:

For verifying identity	For verifying proof of address
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.	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.

Annexure V

Small Accounts:

If an individual customer does not possess either any of the Officially Valid Documents or the documents applicable in respect of simplified procedure, then 'Small Accounts' may be opened for such an individual.

A 'Small Account' means a savings account in which:
• the aggregate of all credits in a financial year does not exceed Rs.100,000;
• the aggregate of all withdrawals and transfers in a month does not exceed Rs.10,000 and
• the balance at any point of time does not exceed rupees fifty thousand, provided, that this limit on balance shall not be considered while making deposits through Government grants, welfare benefits and payment against procurements

A 'small account' maybe opened on the basis of a self-attested photograph and affixation of signature or thumb print. Such accounts may be opened and operated subject to the following conditions:

a) the designated officer of the bank, while opening the small account, certifies under his signature that the person opening the account has affixed her/his signature or thumb print, as the case may be, in her/his presence;

b) a small account shall be 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 and 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;

c) a small account shall remain operational initially for a period of twelve months, and thereafter for a further period of twelve months if the holder of such an account provides evidence before the banking company of having applied for any of the officially valid documents within twelve months of the opening of the said account, with the entire relaxation provisions to be reviewed in respect of the said account after twenty four months;

d) a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism activity or other high risk scenarios, the identity of the customer shall be established through the production of "officially valid documents" and

e) foreign remittance shall not be allowed to be credited into a small account unless the identity of the customer is fully established through the production of "officially valid documents".

Annexure VI

Risk Assessment Table

Individual Customer:

Customer is a PEP or owns a casino, gaming, defense related business, money changing business, remittance agency, etc.	Customer is residing in a high risk jurisdiction	Customer is a citizen of a high risk jurisdiction	Customer owns high risk business	Risk Rating	Due Diligence Process	Full KYC & Periodical Updation of Data
Yes	Regardless	Regardless	Regardless	High	Enhanced DD	Annual
No	Any 2 or more factors are high			High	Enhanced DD	Annual
No	Any one factor is high			Medium	Enhanced DD	Once in 3 years
No	No	No	No	Low	Standard DD	Once in 5 years
No	Yes	No	No	Low	Standard DD	Once in 5 years

Non-Individual Customer:

Customer is: owned/controlled by a PEP or a casino, gaming, defence related business, money changing, remittance agency, etc.	Customer is incorporated in high risk jurisdiction	Customer is operating in high risk jurisdiction	Customer is operating high risk business	Risk Rating	Due Diligence Process	Full KYC & Periodical Updation of Data
Yes	Regardless	Regardless	Regardless	High	Enhanced DD	Annual
No	Any 2 or more factors are high			High	Enhanced DD	Annual
No	No	No	No	Low	Standard DD	Once in 5 years

A periodical review of risk categorization of accounts is to be carried out and enhanced due diligence measures need to be applied wherever required. All accounts need to be scanned through `WorldCheck'. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months. This should be carried out by the concerned Relationship Manager and Head - Branch Ops.