KYC/AML PolicyMarch 2015

March 2015

FEDERAL BANK
YOUR PERFECT BANKING PARTNER

[Company]

TABLE OF CONTENTS

PART A

PART B

ANNEXURES

Abbreviations used

Sl. No.	Abbreviation	Description
1	AML	Anti-Money Laundering
2	AOF	Account Opening Form
3	AWB	Any Where Banking
4	CCR	Counterfeit Currency Report
5	CDD	Customer Due Diligence
6	CEO	Chief Executive Officer
7	CFT	Combating Financing of Terrorism
8	CIF	Customer Information Form
9	CPC	Central Processing Centre
10	CST /VAT	Central Service Tax/ Value Added Tax
11	CTR	Cash Transaction Report
12	CWTR	Cross-border Wire Transfer Report
13	DGFT	Director General of Foreign Trade
14	DMS	Document Management System
15	FATF	Financial Action Task Force
16	FCRA	Foreign Contribution (Regulation) Act
17	FEMA	Foreign Exchange Management Act
18	FI	Financial Institutions
19	FIU-IND	Financial Intelligence Unit -India
20	FPI	Foreign Portfolio Investors
21	HUF	Hindu Undivided Family
22	IEC	Importer Exporter Code
23	KYC	Know Your Customer
24	MHA	Ministry of Home Affairs
25	ML/TF	Money Laundering/ Terrorist Financing
26	MLM	Multi Level Marketing
27	NCCT	Non Cooperative Countries and Territories
28	NEFT	National Electronic Fund Transfer
29	NGO	Non Government Organization
30	NPO	Non Profit Organization
31	NRE	Non Resident External
32	NREGA	National Rural Employment Guarantee Act
33	NRO	Non Resident Ordinary
34	NTR	Non Profit Organization Transaction Report
35	PAN	Permanent Account Number
36	PEP	Politically Exposed Person
37	PIS	Portfolio Investment Scheme
38	PMLA	Prevention of Money Laundering Act
39	RBI	Reserve Bank of India
40	RTGS	Real Time Gross Settlement
41	SEBI	Securities Exchange Board of India

42	STR	Suspicious Transaction Report
43	UAPA	Unlawful Activities (Prevention) Act
44	UCIC	Unique Customer Identification Code
45	UIDAI	Unique Identification Authority of India
46	UN	United Nations
47	UNSCRs	United Nations' Security Council Resolutions
48	UTI	Unit Trust of India

Part A

POLICY ON 'KNOW YOUR CUSTOMER' STANDARDS AND 'ANTI MONEY LAUNDERING' MEASURES

1. Statement of Policy, Purpose & Objectives

1.1 Preamble

In terms of the guidelines issued by Reserve Bank of India on November 29, 2004 on KYC Standards and AML Measures, bank shall put in place a comprehensive policy framework covering KYC standards and AML measures. The guidelines issued by RBI take into account the recommendations made by the Financial Action Task Force (FATF) on AML Standards and on Combating of Financing of Terrorism (CFT). The guidelines also incorporate aspects covered in the Basel committee document on Customer Due Diligence (CDD) measures, which is a reflection of the international financial community's resolve to assist law enforcement authorities in combating financial crime.

The Government of India set up Financial Intelligence Unit – India as an independent body to report directly to the Economic Intelligence Council headed by the Finance Minister. FIU-IND has been established as the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspicious financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

This policy document is prepared in line with the RBI guidelines and incorporates the bank's approach to customer acceptance, customer identification procedures, customer profiling based on the risk perception and monitoring of transactions on an ongoing basis.

1.2 Policy Background

The KYC/AML policy was originally approved by the Board vide BR No. 13/A04/631 dated 18.02.2005, and reviewed periodically thereafter. The last such review was approved by the Board on 27.04.2013

The following guidelines issued by the Reserve Bank of India have been considered as key reference points while reviewing this policy.

i. Master Circular – Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards / Combating of Financing of Terrorism (CFT) / Obligation of banks under PMLA, 2002.

ii. Amendments issued from time to time by IBA, FIU-India and RBI including changes as per the fourth bi-monthly monetary policy statement, 2014-15.

1.3 Policy Objectives

i. To prevent criminal elements from using the Bank for money laundering activities.

ii. To enable the Bank to know/understand the customers and their financial dealings better, which in turn shall help the Bank to manage risks prudently.

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

iv. To comply with applicable laws and regulatory guidelines.

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

1.4 Policy Requirements

To ensure Customer Acceptance Policy, Customer Identification Procedures, Monitoring of Transaction and Risk Management in a prudent manner and thereby preventing occurrence of money laundering and fraud in the bank.

1.5 Scope of the Policy

This policy is applicable to all branches and offices of the bank and its banking/financial subsidiaries and is to be read in conjunction with related guidelines issued from time to time. The guidelines issued up to 31/12/2014 are updated in the annexure – B, which also forms a part of the policy.

1.6 Custodian of the Policy

Integrated Risk Management Department shall be the custodian of the KYC/AML Policy.

1.7 Modification and Review

The policy shall be reviewed periodically (at least once in a Financial Year) incorporating changes needed in view of the amendments issued from time to time by RBI , IBA and FIU-India. The KYC/AML Policy shall be updated and submitted for review to the Risk Management Committee (RMC) and thereafter to the Board of Directors, for final approval.

1.8 Disclosure

The KYC/AML Policy shall be disseminated among all departments, offices and branches for complying KYC/AML standards.

2. Definitions

2.1 Definition of Customer

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

i. A person or entity that maintains an account and/or has a business relationship with the bank
ii. One on whose behalf the account is maintained (i.e. the beneficial owner)

-'Beneficial Owner' means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercise ultimate effective control over a juridical person.

iii. Beneficiaries of transactions conducted by professional intermediaries, such as stock brokers, chartered accountants, solicitors etc as permitted under the law.
iv. Any person or entity connected with a financial transaction that can pose significant reputational or other risks to the bank.

2.2 Definition of Money Laundering

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

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

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

The main objective of the money launderer is to transform 'dirty' money into seemingly clean money or other assets in a way to leave as little trace as possible of the transformation.

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

2.2.1. Stages of Money Laundering

There are essentially three recognized stages of the money laundering process viz. placement, layering and integration.

i. **Placement:** For criminals this is the most vulnerable step in the 'washing' cycle. This is the physical immersion of the criminally derived funds into the financial system. Examples are:

a) Use cash to buy a bank draft to pay into a bank account.
b) Transfer cash to another country by wire transfer.
c) Use the cash to buy traveller's cheques or foreign exchange.
d) Buying a house, car, antique etc.

ii. **Layering:** The physical disposal of cash, which starts to break the link with the original crime by placing money back into the economy. The purpose of layering is to disassociate the illegal monies from the source and perpetrator of the crime by purposely creating a complex web of financial transactions aimed at concealing any audit trail. Examples are:

a) Send the money by wire transfer to other countries, to different people, to a variety of accounts in a variety of currencies.

b) Buy shares, which can be sold.
c) Transfer money to an offshore account etc.

The criminal tries to pass the money through as many layers as possible. Successful layering results in the money being returned to the economy in what appears to be legitimate business funds.

iii. **Integration:** The stage at which the money is integrated into the legitimate economic and financial system and is assimilated with all the other assets in the system. At this stage it becomes virtually impossible to distinguish between 'respectable' and 'dirty' money.

Examples: Purchase of fast food outlets or prime real estate or other cash intensive businesses/properties.

In basic terms, the money launderer wants to:

a) Place money in the financial system, without arousing suspicion
b) Move money around, often in a series of complex transactions crossing multiple jurisdictions, so it becomes difficult to identify its original source, and
c) Move the money back into the financial and business system so that it appears as legitimate funds or assets.

2.2.2. Methods of Money Laundering

There are as many methods to launder money as the imagination allows, and the schemes being used are becoming increasingly sophisticated and complicated as technology advances. The following are some examples of common money laundering methods.

i. **Nominees:** This is one of the most common methods of laundering and hiding assets. A launderer uses family members, friends or associates who are trusted within the community, and who will not attract attention, to conduct transactions on their behalf. The use of nominees facilitates the concealment of the source and ownership of the funds involved.

ii. **Structuring or "smurfing":** Many inconspicuous individuals deposit cash or buy bank drafts at various institutions, or one individual carries out transactions for amounts less than the amount that must be reported to the government, and the cash is subsequently transferred to a central account. These individuals commonly referred to as "smurfs," normally do not attract attention as they deal in funds that are below reporting thresholds and they appear to be conducting ordinary transactions.

iii. **Asset purchases with bulk cash:** Individuals purchase big-ticket items such as cars, boats and real estate. In many cases, launderers use the assets but distance themselves from these by having them registered in a friend or relative's name. The assets may also be resold to further launder the proceeds.

iv. **Exchange transactions:** Individuals often use proceeds of crime to buy foreign currency that can then be transferred to offshore bank accounts anywhere in the world or converted into foreign currency drafts/traveller's cheques.

v. **Currency smuggling:** Funds are moved across borders to disguise their source and ownership and to avoid being exposed to the law and systems that record money entering into the financial system. Funds are smuggled in various ways (such as by mail, courier and body-packing) often to countries with strict bank secrecy laws.

vi. **Gambling in casinos:** Individuals bring cash to a casino and buy gambling chips. After gaming and placing just a few bets, the gambler redeems the remainder of the chips and requests a casino cheque.

vii. **Hawalas/Hundi/Chit (Informal money transfer businesses):** Informal networks that move money on a trust- based pact, with next to no record keeping or formal paper trails. Usually family/clan based front companies/businesses are popular with cultures that don't use or trust formal banking. Millions of dollars/other foreign currencies change hands globally through this route.

2.2.3. Money Laundering - Risk Perception

The Bank is exposed to the following risks, which arise out of Money Laundering activities:

i. **Reputation Risk**

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

ii. **Compliance Risk**

Risk of loss due to failure of compliance with key regulations governing the bank's operations.

iii. **Operational Risk**

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

iv. **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.

2.2.4. Money Laundering Risk Assessments

The level of Money Laundering risks that the Bank is exposed to by a customer relationship depends mainly on:

i. Type of the customer and nature of business

ii. Type of product/service availed by the customer

iii. Country where the customer is domiciled

Risks are increased if the money launderer can hide behind corporate structures such as limited companies, offshore trusts, special purpose vehicles and nominee arrangements.

2.2.5. Offences and Penalties

Failure to comply with the Anti-Money Laundering regulations constitutes an offence and those not complying with the law will find their reputation severely damaged and details of the offence published in the local/national/international press. Bank should therefore comply with the established laws and regulations in order to protect our good name and reputation, decrease the likelihood of becoming a victim of fraud or illegal activity, and ensure safe and sound business practices for our customers. In keeping with our goodwill, mission, values and policy, to ensure compliance with the law, and to prevent abuse of our facilities Bank shall observe the government laws and refuse to aid those who attempt to evade them. In order to prevent the name of the bank being dragged into any unpleasant situations/circumstances, branches/offices shall observe the following guidelines.

It shall be noted that there are substantial civil and criminal penalties for willful and negligent failure to comply with anti-money laundering laws and regulations. Failure to comply may result in imposition of fines, criminal charges and significant jail terms. These laws are in place for bank's protection; they also aid in the fight against terrorism and criminal activity derived from

the proceeds of crime, and they are not to be taken lightly. Hence every branch/office/employee must be aware that criminal liability may be imposed on themselves and the bank, if we are willfully blind to suspicious activity or we should have known that the activity was suspicious. There are three principal criminal offences relating to money laundering activities by, through, or to a financial institution. These offences can be classified as follows.

i. Knowingly helping launder money from criminal activity.

ii. Knowingly engaging (including by being willfully blind) in a transaction that involves property from criminal activity.

iii. Structuring transactions to avoid reporting and record keeping requirements.

3. Key Elements of the Policy

3.1 Customer Acceptance Policy

The customer acceptance policy shall provide explicit criteria for the acceptance of customers. Accordingly,

i. Bank should not allow the opening of or keep any anonymous account or accounts in fictitious name or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

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

iii. Accept customers after verifying their identity as laid down in Customer Identification Procedures.

iv. Necessary checks shall be undertaken 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.

v. Classify customers into risk categories - Low, medium and high based on risk perception, which includes parameters like nature of business, location, social and financial status etc (Criteria for each category of customers detailed in Annexure F).

vi. Bank should prepare a profile for each new customer based on risk categorisation. 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 banks should take care to seek only such information from the customer, which is relevant to the risk category and is not intrusive.

vii. 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.

viii. Not to open an 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-reliability of the data / information furnished to the bank.

ix. Adhere to any other internal instructions given from time to time

x. While carrying out due diligence, the bank shall ensure that the procedure adopted will not result in denial of banking services to the general public especially those who are financially or socially disadvantaged.

3.2 Customer Identification Procedures

Customer identification means identifying the customer and verifying his / her identity by using reliable, independent source documents, data or information. Bank should obtain sufficient information necessary to establish, to its 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 should 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. Besides risk perception, the nature of information / documents required would also depend on the type of customer risk profile (individual, corporate etc).

The information collected should be used for profiling the customer. Wherever applicable, information on the nature of business activity, location, mode of payments, volume of turnover, social and financial status etc shall be collected for completing the profile of the customer. The information collected from the customer as for the identification process shall be treated as confidential and details thereof shall not be divulged for cross selling or any other purposes. Customer Identification Procedures shall also be carried out in respect of non-account holders approaching for high value one-off transaction. Customer identification requirements in respect of a few typical cases, especially, legal persons require an extra element of caution like Trust, Companies, non-face-to-face customers etc.

Identity to be verified for -

i. The named account holder
ii. Beneficial owners
iii. Signatories to an account and
iv. Intermediate parties.

The Customer Identification Procedures are to be carried out at the following stages.

i. While establishing a banking relationship
ii. Periodically as part of KYC review or when the bank feels it is necessary to obtain additional information from the existing customers based on the conduct or behaviour of the account.

Customers shall be classified into three risk categories namely 'High', 'Medium', 'Low' based on the risk perception. The risk categorization will be reviewed periodically once in six months. The customers shall be allotted with a “unique customer identification code” (UCIC) for tracking the various facilities availed and monitor financial transactions in a holistic manner.

3.2.1 Proof of Address

If the address on the document submitted for identity proof by the prospective customer is same as that declared by him/her in the account opening form, the document should be accepted as a valid proof of both identity and address.

Bank shall allow customers to submit only one documentary proof of address (either current or permanent) while opening a bank account or while undergoing periodic updation. In case the address mentioned as per ‘proof of address’ undergoes a change, fresh proof of address shall be submitted to the branch within a period of six months. In case the proof of address furnished by the customer is not the local address or address where the customer is currently residing, the bank shall take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence/local address. This address should be verified by the bank through ‘positive confirmation’ such as acknowledgment of receipt of (i) letter, cheque books, ATM cards; (ii) telephonic conversation; (iii) visits; etc. In the event of change in this address due to relocation or any other reason, customers shall intimate the new address for correspondence to the bank within two weeks of such a change.

Some close relatives, e.g. wife, son, daughter and parents etc. who live with their husband, father / mother and son, may find it difficult to open account as the documents required for address verification are not in their name. In such cases, bank shall obtain an identity/address

document of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (Prospective customer) desiring to open an account is a relative and is staying with him / her. Bank shall use supplementary evidence such as a letter received through post for further verification of the address.

3.2.2 Transfer of Accounts within Bank

KYC once done by one branch of the bank should be valid for transfer of the account within the bank as long as full KYC has been done for the concerned account. The customer shall be allowed to transfer his account from one branch to another branch without restrictions. Bank may transfer existing accounts at the transferor branch to the transferee branch without insisting on fresh proof of address and on the basis of a self-declaration from the account holder about his/her current address.

3.2.3 Periodical updation of KYC information

Bank should carry out periodical updation of KYC information of every customer, which shall include the following:

i. Full KYC exercise shall be done at least every two years for high risk customers, every eight years for medium risk customers and every ten years for low risk customers. Full KYC shall include all measures for confirming identity and address and other particulars of the customer that the bank shall consider reasonable and necessary based on the risk profile of the customer.

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

iii. If an existing KYC compliant customer desires to open another account, there is no need for submission of fresh proof of identity/address.

iv. Fresh photographs should be obtained from minor customer on becoming major.

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

While the KYC guidelines will apply to all new customers, the same shall also be applied to the existing customers on the basis of materiality and risk. Bank shall impose partial freezing on existing KYC non-compliant accounts after giving due notice.

An indicative list of the nature and type of documents/information that shall be relied upon for customer identification is given in Annexure A.

3.2.4 Relaxation in norms – Small Accounts

In order to facilitate the backward and socially disadvantaged section of the people who do not have any KYC documents for opening Bank accounts and also in connection with financial inclusion mission, Government of India has amended the Prevention of Money Laundering Rules, 2005, and has introduced separate procedure for opening ‘small accounts’ by customers.

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

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

Accordingly, bank shall allow an individual who desires to open a “small account” on production of a self attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account, provided that

i. the bank official shall certify under his signature that the person opening the account has affixed his signature or thumb print, as the case may be, in his presence
ii. a small account shall be opened only at Core Banking Solution linked banking company branches or in a branch where it is possible to manually monitor and ensure that foreign remittances are not credited to a small account and that the stipulated limits on monthly and annual aggregate of transactions and balance in such accounts are not breached, before a transaction is allowed to take place
iii. 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.
iv. a small account shall be monitored and when there is suspicion of money laundering or financing of terrorism or other high risk scenarios, the identity of client shall be established through the production of officially valid documents.
v. Foreign remittance shall not be allowed to be credited into a small account unless the identity of the client is fully established through the production of officially valid documents.

3.2.5 Operation of Bank Accounts & Money Mules

“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.

In a money mule transaction, an individual with a bank 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 are generally 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 bank 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.

Normally these types of transactions will be done without giving much chance for any suspicion. The nature of transaction and the awareness about the true profile of the customer only help to track such accounts. Ongoing close monitoring of transactions and the periodical updation of customer identification data after the account is opened are the main tools to identify such accounts. Transactions in dormant account, unused salary accounts and current accounts opened in individual names are prone to such transactions.

In order to prevent and minimise the operations of such mule accounts, branches/offices shall follow the guidelines on opening of accounts and monitoring of transactions.

3.3 Monitoring of Transactions

Ongoing monitoring is an essential element of effective KYC procedures. Bank shall effectively control and reduce the risk by having an understanding of the normal and reasonable activity of the customer so as to identify the transactions that fall outside the regular pattern of activity. The extent of monitoring shall depend on the risk sensitivity of the account. Special attention shall be given to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose. Bank shall prescribe threshold limits for a particular category of accounts and pay particular attention to the transactions which exceed these limits.

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. High-risk accounts shall 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) & jewellers should be taken into account to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to Financial Intelligence Unit- India (FIU-IND).

Bank shall put in place a system of periodical review of risk categorization of accounts for applying enhanced due diligence measures as mentioned in para 3.4.1. Such review of risk categorisation of customers should be carried out at a periodicity of not less than once in six months.

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.

The risk categorization of customers as also compilation and periodic updation of customer profiles and monitoring and closure of alerts in accounts by banks are extremely important for effective implementation of KYC/AML/CFT measures. Branches/Offices should, therefore, ensure compliance with the regulatory guidelines on KYC/AML/CFT both in letter and spirit.

3.3.1 Accounts of Multi-level Marketing Companies

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 honoured but once the chain breaks, all such post-dated instruments are dishonoured. This results in fraud on the public and is a reputational risk for banks concerned.

Bank should 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, bank shall carefully analyse such data and in case they find unusual operations in accounts, the matter shall be immediately reported to Reserve Bank and other appropriate authorities such as Financial Intelligence Unit India (FIU-Ind) under Department of Revenue, Ministry of Finance.

Bank should be more careful in opening and operating accounts for such schemes specifically verifying the type of business and inherent risk associated with such activity. Bank will be held

responsible for losses incurred by customers by way of deposits in / remittance from such accounts if they are found to be in violation of regulations and failure to adhere to the regulatory restrictions will invite supervisory action.

3.3.2 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, bank shall consider closing the account or terminating the banking/business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions shall be taken at a reasonably senior level. Accordingly, Zonal Head shall take the decision on a case to case basis.

3.4 Risk Management

The Bank shall adopt a risk-based approach to ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. Bank should establish appropriate framework covering proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility should be explicitly allocated within the bank for ensuring that the bank's policies and procedures are implemented effectively. Bank should adhere the following for the effective implementation of risk management.

i. Bank's Inspection Department shall ensure that the internal inspections provide an independent evaluation of compliance of KYC / AML policy including legal and regulatory requirements.

ii. Concurrent auditors shall specifically check and verify the application of KYC/AML procedures at the branches and offices of the Bank and comment on the lapses observed in this regard.

iii. Adverse features noted by the internal/concurrent auditors shall be brought to the attention of the Principal Officer.

iv. Compliance of the above stipulations shall be put before the Audit Committee of the Board by the Inspection Department at quarterly intervals.

v. Review of implementation of KYC / AML Guidelines shall also be put before the Audit Committee of the Board by AML Cell at quarterly intervals.

vi. The Bank shall have an on-going employee-training programme so that members of the staff are adequately trained in KYC/AML procedures.

vii. The Principal Officer designated by the Bank in this regard shall have responsibility in managing oversight and coordinating with various functionaries in the implementation of KYC/AML Policy.

viii. Designated Director shall be responsible for the overall compliance with the obligations under the Act and Rules.

Bank shall 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.

As and when negative list of individuals and entities, approved by Security Council Committee established pursuant to various United Nations' Security Council Resolutions (UNSCRs), is received from Government of India, AML cell shall ensure to update the lists of individuals and entities as circulated by Reserve Bank to scan against the existing accounts and the new accounts to be opened on a daily basis.

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. Bank shall gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Such relationships shall be established only with the approval of the Board or by MD & CEO committee subject to subsequent approval of the Board in the next meeting.

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 may be of special relevance. Also it shall be ascertained from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. Such relationships should be established only with the approval of the Board.

In the case of arrangements with co-operative banks wherein the latter open current accounts with us and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for facilitating their remittances and payments, bank should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising there from. For this purpose, bank should 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.

Bank shall not enter into a correspondent relationship with a "shell bank" (i.e. a bank which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group). Shell banks are not permitted to operate in India.

Wire transfer is an instantaneous and most preferred route for transfer of funds across the globe and hence, it shall be ensured that terrorists and other criminals are prevented from having unfettered access to wire transfers for moving their funds. Accordingly, bank shall be prepared to provide the basic information on the originator of wire transfers 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, whenever necessary.

3.4.1 Risk Rating

The risk related to an account / customer other than NRIs shall be arrived at based on ten risk parameters as listed below. Bank shall apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence', especially for high risk categorized customers.

Sl. No	Risk Parameters
1	Product code
2	Country Code
3	Customer Type
4	Mode of Operation
5	Source of Funds
6	Customer occupation
7	Net worth
8	Account status
9	Average Monthly Turnover

10	STR(Suspicious Transactions Report) filed cases

The detail of individual risk parameters is given in Annexure D.

As per the clarification from RBI dated 02.01.2015, banks are allowed to take a view on risk categorization of each customers into Low, Medium and High risk category based on their assessment and risk perception of the customers, and not merely based on any group or class they belong to such as Non Resident customers, bullion dealers and high net worth individuals.

In this context, Bank shall arrive at the risk category of NRI customers on the basis of eleven risk parameters which is detailed in Annexure D1.

The accounts shall be rated at regular periodic intervals with the help of necessary software/solutions. Customer Risk shall be arrived from the account risk. The maximum amongst the risks of all the accounts of a customer shall be treated as the risk of the customer.

4. Designated Director and Principle Officer

a) Designated Director

Bank shall nominate a Director on their 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. Accordingly, MD&CEO shall be nominated as the Designated Director as per the provisions.

b) Principal Officer

Bank shall appoint a senior management officer to be designated as Principal Officer. Bank 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 shall 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 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 form time to time. The Principal Officer shall also be responsible for timely submission of CTR, STR, NTR, CCR and CWTR, to FIU-IND.

To enable 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. Head of Operational Risk Management Division, IRMD shall be designated as the Principal Officer as per the provisions.

5. Maintenance of records/ transactions reporting to Financial Intelligence Unit-India (FIU-IND)

Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Accordingly, the bank shall maintain/report the following in this regard.

5.1 Maintenance of records of transactions

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

i. All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

ii. All series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh;

iii. All transactions involving receipts by non-profit organisations of value more than Rupees Ten Lakh or its equivalent in foreign currency;

iv. 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

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

5.2 Information to be preserved

Bank shall maintain all necessary information in respect of transactions referred to in PML Rule 3 to permit reconstruction of individual transaction, including the following information:

i. the nature of the transactions;

ii. the amount of the transaction and the currency in which it was denominated;

iii. the date on which the transaction was conducted; and

iv. the parties to the transaction.

5.3 Maintenance and Preservation of Records

Bank shall maintain the records containing information of all transactions including those mentioned in para 5.1 above. Account information shall be preserved in a manner that allows data to be retrieved easily and quickly whenever required or when requested by the competent authorities. All necessary records of transactions, both domestic or international, shall be maintained for at least five years from the date of transaction, which will enable 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.

Bank shall 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, 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. The identification records and transaction data shall be made available to the competent authorities upon request.

5.4 Reporting to Financial Intelligence Unit – India

Bank shall report information relating to cash and suspicious transactions, transactions involving counterfeit currency, cross border wire transfers and all transactions involving receipts by non-profit organisations of value more than Rupees Ten Lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND).

The alerts on suspicious transactions shall be generated daily on the basis of predefined benchmarks and initially examined at AML Cell. The transactions, which require further details, shall be taken up with concerned branches by seeking additional details / clarifications / compliance.

5.4.1 Various Reporting Formats

i. **Cash Transaction Report (CTR)**

All cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency or all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds Rupees Ten Lakh should be submitted in the prescribed format to FIU-IND by 15th of the succeeding month.

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.

ii. **Suspicious Transaction Reports (STR)**

Bank 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.

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.

The STR should be furnished within seven 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.

iii. **Non-Profit Organisation Transaction Reports (NTR)**

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

iv. **Cross-border Wire Transfer Report (CWTR)**

Cross-border Wire Transfer Report (CWTR) should be submitted 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 fund is in India.

v. **Counterfeit Currency Reports (CCR)**

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 by 15th of the succeeding month in the prescribed format. 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.

Branches shall report any such transactions detected during the course of their business to AML Cell, IRMD on the day of occurrence itself in the specified format (Refer Annexure E). A separate Counterfeit Currency Report (CCR) should be filed for each incident of detection of counterfeit Indian Currency. If the detected counterfeit currency notes can be segregated on the basis of tendering person, a separate CCR should be filed for each such incident.

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

6.1 Customer Education

Implementation of KYC procedures requires bank to demand certain information from customers which may be of personal nature or which have 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. Accordingly bank shall prepare specific literature/ pamphlets etc. so as to educate the customer of the objectives of the KYC programme. The front desk staff shall be specially trained to handle such situations while dealing with customers.

6.2 Employees' Training

Bank shall 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.

6.3 Hiring of Employees

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