IIBF & NISM Adda

Certificate Examination in

Anti-Money Laundering & Know Your Customer

2019

Compiled by

Srinivas Kante B.Tech, CAIIB

About Certificate Examination in Anti-Money Laundering & Know Your Customer

IIBF Certificate Examination

Objective:

To provide advanced knowledge and understanding in AML / KYC standards and to develop the professional competence of employees of banks and financial institutions

Eligibility

Employees of Banks / NBFCs / Financial Institutions / Insurance Companies etc. are eligible to write the examination.

EXAMINATION FEES / REGISTRATION FEE

For Members For Non-Members
First attempt `1,124/- * `1,685/- *

Subsequent each attempt `1,124/- * `1,685/- *

Examination will be conducted in English only.
(i) Each Question Paper will contain approximately 120 objective type multiple choice questions.
(ii) The examination will be held in online mode only. A list of examination centre will be provided in the online examination application form.
The duration of the examination will be of two hours.
(i) The examination will be conducted normally twice a year in May / June andNovember / December.
(ii) Examination **will be conducted on a Sunday.**
Candidate has to secure 60% or more marks in the examination to pass i.e. 60 marks out of 100.
Application for examination should be made online from the Institute's website **www.iibf.org.in**. No physical form will be accepted by the Institute with effect from 1st January, 2013.
Non-members applying for Institute's exams / courses are required to submit a copy of any one of the following documents along with Examination Application
Form. Forms without the same shall be liable to be rejected.
1) Photo i/card issued by Employer or 2) PAN Card or 3) Driving License or 4) Election Voter's i/card or 5) Passport or 6) Aadhaar Card
The Institute has developed a courseware to cover the syllabus. Candidates are advised to make full use of the courseware and also the updates put on the IIBF website from time to time. However, as banking and finance fields are dynamic, rules and regulations witness rapid changes. Hence, candidates should keep themselves updated on latest developments by going through Master Circulars issued by RBI, visiting the websites of organizations like RBI, SEBI, BIS etc.
The Institute has published study books to facilitate study and they will be available at outlets / showrooms / distributors of M/s. Macmillan Publishers India Ltd.

SYLLABUS

(I) ANTI MONEY LAUNDERING

Money Laundering - Origin - Definition - Techniques Impact on Banks - Structuring; Integration, Preventive Legislations - International Co-operation - UK; USA; India - Basel Committee - PMLA Objectives - RBI Guidelines - System Adequacy to Combat Money Laundering - Antiterrorism finance - Financial Intelligence Unit (FIU) The Financial Action Task Force (FATF) - IBA Working Group - Software for AML Screening : Money Laundering and Correspondent Banking - Exchange Companies - Foreign Branches

(II) KNOW YOUR CUSTOMER - INTRODUCTION AND OVERVIEW

Customer Profile - KYC Policies - Countries Deficient in KYC Policies,nInitiatives by the RBI - Organised Financial Crimes Customer - Definition under the KYC Principles - Transaction Profile - Organisational Structure – Important KYC framework in RBI prescriptions - Operating Guidelines. Introduction of new accounts - Guidelines for Opening Accounts of Companies, Trusts, Firms, Intermediaries etc., Client Accounts opened by Professional Intermediaries - Trust / Nominee or Fiduciary Accounts - Accounts of Politically Exposed Persons (PEPs) Residing Outside India, Accounts of 'non-face-to-face' Customers - Qualitative data - Joint accounts - Minor accounts - KYC for existing accounts - KYC for low income group customers. Monitoring Accounts - Customer research - Suspicious transactions

INDEX

1 PREFACE

This policy and procedure document is a comprehensive source of reference for all the concerned and relevant activities of the Bank towards Know Your Customer (KYC), Anti Money Laundering (AML) and Combating the Financing of Terrorism (CFT) compliance. The policies and procedures developed are designed to ensure that the Bank is committed to the prevention of the use of its facilities for laundering the proceeds of crime and financing terrorist activities. It consists of the following sections:

− Risk based acceptance model to facilitate the classification of current and existing customers on the basis of money laundering and terrorist financing risk;
− Account opening procedures including customer classification, verification of customer information using documentary and non-documentary methods and escalation processes;
− Policy for customer information updates based on the risk level of the individual or entity;
− Internal controls to measure the risk levels of products, services and customers accepted and to measure the effectiveness of current policies and procedures;
− Policies and procedures for the monitoring and reporting of transactions;
− Policies and procedures for customer record maintenance, retention and their sharing with government agencies; and
− Recommendation for a training programme for Bank officials geared towards customer identification and acceptance, customer risk ranking and detection of money laundering instances.

1.1 Statement of commitment

The goals and objectives of this KYC, AML & CFT programme are to (1) deter individuals and entities from using the Bank to launder the proceeds of illegal activities; (2) enable member branches of the Bank to comply with their obligations under the Prevention of Money Laundering Act, Unlawful Activities Prevention Act (ULPA) and regulations from Reserve Bank of India (RBI) and National Bank for Agriculture and Rural Development (NABARD), regulatory bodies for the banks; (3) manage and mitigate money laundering and terrorist financing related risks; (4) allow banks to cooperate with regulatory bodies and government agencies in detecting and deterring money laundering and terrorist financing; and (5) provide employees with guidance for actions to be taken to comply with the Bank's obligations under the law and the Bank's policies.

2 Definitions

2.1 Customer

RBI defines a customer1 as any one of the following:

− A person or entity that maintains an account and/or has a business relationship with the Bank.
− One on whose behalf the account is maintained (i.e., the beneficial owner) or beneficiary of transactions conducted by professional intermediaries, such as stock brokers, chartered accountants, solicitors, etc. as permitted under the law.
− Any person or entity connected with a financial transaction or any other product offered by the Bank including walk-in customers.

2.2 High Net-Worth Individual

An individual is designated as a High Net-Worth Individual (HNI) for the purposes of the Bank if the sum of all the credits for the individual at the Bank across all products exceeds Rupees 15 lakhs (Rs. 15,00,000)

2.3 Beneficial Owners

The Beneficial Owner for an entity constitution type is any individual or entity that owns or controls over 20% of the entity. For an individual constitution type the beneficial owner refers to the individual itself or all the operators of the account.

2.4 Controlling Parties

Controlling parties are individuals or entities with direct or indirect control over the account created. For KYC purposes, the controlling parties are defined as authorized signatories, power of attorney holders, executive management (e.g. CEO, CFO, Directors) and Board of Directors. Different account types and transactions could involve different controlling parties.

2.5 Money Laundering

Money Laundering is a process by which illegal sources of money are disguised to make it appear as if they were the proceeds of legal activities. It usually occurs in three steps:

1. The placement step involving the introduction of the money into the financial system;
2. The second step known as layering involves performing complex financial transactions to hide the illegal source; and

3. Finally, the integration step, during which the previously illegal proceeds enter the economy and are converted into apparently legitimate earnings.

2.6 Terrorist Financing

Terrorist Financing relates to the use of financial institutions to launder money or misdirect clean money for illegal and illegitimate terrorist activities. Terrorist financing, unlike money laundering, cares little about the source of the funds and its purpose is what defines the scope.

2.7 Small Account

A small account refers to a savings bank account where:

1. The aggregate of all credits in a financial year does not exceed Rupees one lakh (Rs. 1,00,000);
2. The aggregate of all withdrawals and transfers in a month does not exceed Rupees ten thousand (Rs. 10,000); and
3. The balance at any point of time does not exceed Rupees fifty thousand (Rs. 50,000)

2.8 Financial Intermediary

For the purposes of this document, a financial intermediary is a person or institution that acts on behalf of its customers to conduct a transaction or open an account with the Bank.

As per the RBI, the term Financial Intermediary includes following persons or entities registered under Section 12 of the Securities and Exchange Board of India (SEBI) Act,
1992:

1. Stock brokers
2. Sub-brokers
3. Share transfer agents
4. Bankers to an issue
5. Trustees to trust deed
6. Registrars to issue
7. Merchant bankers
8. Underwriters
9. Portfolio Managers
10. Depositories and Participants
11. Custodian of securities
12. Credit rating agencies
13. Venture capital funds
14. Collective investment schemes including mutual funds

2.9 Ordering Bank

In relation with wire transfers, an Ordering Bank is a Bank that originates a wire transfer as per the order placed by its customers

2.10 Intermediary Bank

In relation with wire transfers, an Intermediary Bank provides business services on behalf of another financial institution (ordering and beneficiary bank). Intermediary Banks are also known as Correspondent Banks and are used by domestic banks in order to service transactions originating in different cities, states or foreign countries, and act as a domestic bank's agent. This is done because the domestic bank may have limited access to markets outside of its geography, and cannot service its client accounts without opening up a branch in that particular city, state or country.

2.11 Beneficiary Bank

In relation with wire transfers, a Beneficiary Bank refers to the bank identified in a payment order in which an account of the beneficiary is to be credited pursuant to the order or which otherwise is to make payment to the beneficiary if the order does not provide for payment to an account.

3 Legislative and Regulatory Framework

3.1 Defined legal frameworks

3.1.1 Prevention of Money Laundering Act 2002

The Prevention of Money Laundering Act (PMLA) of 20022 is the legislation that forms the core of the legal framework put in to place to combat money laundering. The PMLA came into effect from 1st July 2005 with two amendments passed in May 2005 and March 2009. The act criminalises money laundering and also provides for freezing and confiscation of assets associated in money laundering. It requires financial institutions and intermediaries to verify the identity of clients, maintain records and furnish prescribed transactional information to the FIU-IND.

3.1.2 Rules under PMLA

In addition, the Government of India has strengthened the PMLA through the notification of various rules, known as Prevention of Money Laundering Rules (PMLR), to enforce the PMLA which includes defining an adjudicating authority and appellate tribunal, conferring exclusive and concurrent powers, specifying rules for receipt and management of confiscated properties, etc. A complete listing of the rules and their purpose is available on the FIU-IND website3

3.1.3 Unlawful Activities (Prevention) Act, 1967

The Unlawful Activities Prevention Act of 1967, amended in 2008, relates to the purposes of prevention, and for coping with terrorist activities. The Government of India has issued an order dated August 27 2009 detailing the procedure for

implementing of section 51A of the Act and it empowers the Central Government 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 in engaged in terrorism ,or

− 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 or Order.

3.2 Applicable Regulatory Authorities

3.2.1 Reserve Bank of India

The RBI is the central banking institution in India and controls the monetary policy of the rupee and the currency reserves. Through its Master Circular on Know Your Customer (KYC) norms/Anti Money Laundering (AML) Standards/Combating of Financing of Terrorism/Obligations of Banks under PMLA, 2002 the RBI introduced KYC guidelines for all banks which it has since updated yearly. The RBI also has the authority to penalize banking institutions for violations in KYC, AML and CFT norms.

3.2.2 National Bank for Agriculture and Rural Development

NABARD is the apex development bank in India and is accredited with matters regarding policy, planning and operations in the field of credit for agriculture and other economic activities in rural regions in India. In discharging its role as a facilitator for rural prosperity, NABARD is also entrusted with acting as a regulator for Cooperative Banks and Regional Rural Banks (RRBs). NABARD created a model KYC policy for its member banks with a stipulation that it be tailored to the individual needs of the bank.

3.2.3 Financial Intelligence Unit – India

FIU-IND is the central national agency responsible for receiving, processing, analysing and disseminating information relating to suspicious financial transactions and is responsible for domestic and global efforts against money laundering and related crimes. Any reports regarding financial transactions such as Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs) must be filed with the agency. FIU-IND also has the authority to request additional information on individuals or entities from banks and other financial institutions.

3.3 Consequences of Non-Compliance

3.3.1 Penalties for Non-Compliance

Any contravention or non-compliance with RBI's instructions relating to KYC, AML and CFT guidelines shall attract penalties under the provisions of Section 47(A) (1) (b) read with Section 46(4) of the Banking Regulation Act, 1949. The RBI has imposed fines on various public and private sector banks for non-compliance with KYC norms. In the first six months of 2011, over 48 cooperative banks had been fined between Rupees one lakh (Rs. 1, 00,000) and Rupees five lakh (Rs. 5, 00,000) for various KYC, AML and CFT related offences. Additionally, the PMLA specifies punishments of up to ten years of rigorous imprisonment on whosoever willingly commits the offence of money laundering.

3.3.2 Reputational Risk

If the Bank is penalised for non-compliance, it can create a negative perception of the institution on customers, investors and regulators and can adversely affect the Bank's ability to raise capital and to maintain and create business relationships. RBI has stepped up its actions against non-compliant banks and in addition to fiscal penalties, also issues notifications and press releases5 on the banks that have been fined for violation of KYC, AML and CFT guidelines. These press releases are picked up by national and international news media which can result in a severe reputational damage to the banks.

SHORT NOTES ON ANTI MONEY LAUNDERING

1. The conversion or transfer of property, the concealment or disguising of the nature of the proceeds, the acquisition, possession or use of property, knowing that these are derived from criminal activity and participate or assist the movement of funds to make the proceeds appear legitimate is money laundering.

Money obtained from certain crimes, such as extortion, insider trading, drug trafficking, and illegal gambling is "dirty" and needs to be "cleaned" to appear to have been derived from legal activities, so that banks and other financial institutions will deal with it without suspicion. Money can be laundered by many methods which vary in complexity and sophistication.

Money laundering involves three steps: The first involves introducing cash into the financial system by some means ("placement"); the second involves carrying out complex financial transactions to camouflage the illegal source of the cash ("layering"); and finally, acquiring wealth generated from the transactions of the illicit funds ("integration"). Some of these steps may be omitted, depending upon the circumstances. For example, non-cash proceeds that are already in the financial system would not need to be placed.[8]

According to the United States Treasury Department:

Money laundering is the process of making illegally-gained proceeds (i.e., "dirty money") appear legal (i.e., "clean"). Typically, it involves three steps: placement, layering, and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean".

2.Money laundering involves taking criminal proceeds and disguising their illegal source in anticipation of ultimately using the criminal proceeds to perform legal and illegal activities.
Simply put, money laundering is the process of making dirty money look clean.

3. **Money laundering methods**

Money laundering:

The money laundering cycle can be broken down into three distinct stages; however, it is important to remember that money laundering is a single process. The stages of money laundering include the:

Placement Stage

Layering Stage

Integration Stage

The Placement Stage

The placement stage represents the initial entry of the "dirty" cash or proceeds of crime into the financial system. Generally, this stage serves two purposes: (a) it relieves the criminal of holding and guarding large amounts of bulky of cash; and (b) it places the money into the legitimate financial system. It is during the placement stage that money launderers are the most vulnerable to being caught. This is due to the fact that placing large amounts of money (cash) into the legitimate financial system may raise suspicions of officials.

The placement of the proceeds of crime can be done in a number of ways. For example, cash could be packed into a suitcase and smuggled to a country, or the launderer could use smurfs to defeat reporting threshold laws and avoid suspicion. Some other common methods include:

Loan Repayment

Repayment of loans or credit cards with illegal proceeds Gambling

Purchase of gambling chips or placing bets on sporting events

Currency Smuggling

The physical movement of illegal currency or monetary instruments over the border

Currency Exchanges

Purchasing foreign money with illegal funds through foreign currency exchanges

Blending Funds

Using a legitimate cash focused business to co-mingle dirty funds with the day's legitimate sales receipts

This environment has resulted in a situation where officials in these jurisdictions are either unwilling due to regulations, or refuse to cooperate in requests for assistance during international money laundering investigations.

To combat this and other international impediments to effective money laundering investigations, many like-minded countries have met to develop, coordinate, and share model legislation, multilateral agreements, trends & intelligence, and other information. For example, such international watchdogs as the Financial Action Task Force (FATF) evolved out of these discussions.

The Layering Stage

After placement comes the layering stage (sometimes referred to as structuring). The layering stage is the most complex and often entails the international movement of the funds. The primary purpose of this stage is to separate the illicit money from its source. This is done by the sophisticated layering of financial transactions that obscure the audit trail and sever the link with the original crime.

During this stage, for example, the money launderers may begin by moving funds electronically from one country to another, then divide them into investments placed in advanced financial options or overseas markets; constantly moving them to elude detection; each time, exploiting loopholes or discrepancies in legislation and taking advantage of delays in judicial or police cooperation.

The Integration Stage

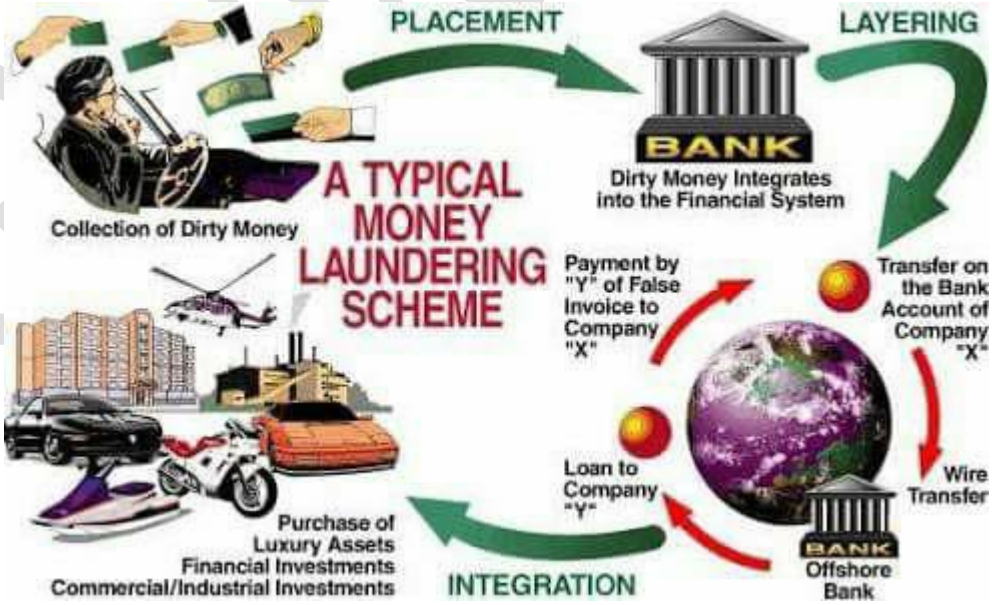
The final stage of the money laundering process is termed the integration stage. It is at the integration stage where the money is returned to the criminal from what seem to be legitimate sources. Having been placed initially as cash and layered through a number of financial transactions, the criminal proceeds are now fully integrated into the financial system and can be used for any purpose.

There are many different ways in which the laundered money can be integrated back with the criminal; however, the major objective at this stage is to reunite the money with the criminal in a manner that does not draw attention and appears to result from a legitimate source. For example, the purchases of property, art work, jewellery, or high-end automobiles are common ways for the launderer to enjoy their illegal profits without necessarily drawing attention to themselves

Smurfs - A popular method used to launder cash in the placement stage. This technique involves the use of many individuals (the"smurfs") who exchange illicit funds (in smaller, less conspicuous amounts) for highly liquid items such as traveller cheques, bank drafts, or deposited directly into savings accounts. These instruments are then given to the launderer who then begins the layering stage.

For example, ten smurfs could "place" $1 million into financial institutions using this technique in less than two weeks

Image from UNODC



3. Case study:

Online or Internet Banking (Special Case study how Money laundering 3 steps Happens):: Very important

Placement — Launderers want to get their proceeds into legitimate repositories such as banks, securities or real estate, with as little trace of the source and beneficial ownership as possible. Often, cyberspace banks do not accept conventional deposits. However,cyberbanks could be organized to take custodial-like forms — holding, reconciling and transferring rights to assets held in different forms around the world. Money launderers can create their own systems shadowing traditional commercial banks in order to acceptdeposits, perhaps as warehouses for cash or otherbulk commodities. Thus, cyberspace banks have thepotential to offer highly secure, uncommonly private"placement" vehicles for money launderersLayering — Electronic mail messages, aided by encryption and cyberspace banking transfers, enablelaunderers to transfer assets around the world manytimes a day.

Integration — Once layered, cyberspace bankingtechnologies may facilitate integration in two ways.If cyberbanking permits person-to-person cash-like transfers, with no actual cash involvement, existing currency reporting regulations do not apply. Using"super smart-card" technologies, money can be movedaround the world through ATM transactions. These smart cards permit easy retrieval of the "account"balance by the use of an ATM card

Terrorism Financing are 3 types

A. State financing: Separate entities are created with organizational and financial support of the state
B. Legimate modes : Donations by business,individuals and charity funds
C. Private funding:by criminal activities by bank robberies, drug trafficking, kidnaps,exortion..

Money laundering can take several forms, although most methods can be categorized into one of a few types. These include "bank methods, smurfing [also known as structuring], currency exchanges, and double-invoicing".

Structuring: Often known as *smurfing*, this is a method of placement whereby cash is broken into smaller deposits of money, used to defeat suspicion of money laundering and to avoid anti-money laundering reporting requirements. A sub-component of this is to use smaller amounts of cash to purchase bearer instruments, such as money orders, and then ultimately deposit those, again in small amounts.

- Bulk cash smuggling: This involves physically smuggling cash to another jurisdiction and depositing it in a financial institution, such as an offshore bank, with greater bank secrecy or less rigorous money laundering enforcement
- Cash-intensive businesses: In this method, a business typically expected to receive a large proportion of its revenue as cash uses its accounts to deposit criminally derived cash. Such enterprises often operate openly and in doing so generate cash revenue from incidental legitimate business in addition to the illicit cash – in such cases the business will usually claim all cash received as legitimate earnings. Service businesses are best suited to this method, as such enterprises have little or no variable costs and/or a large ratio between revenue and variable costs, which makes it difficult to detect discrepancies between revenues and costs. Examples are parking structures, strip clubs, tanning salons, car washes, arcades, bars, restaurants, and casinos.
- Trade-based laundering: This involves under- or over-valuing invoices to disguise the movement of money. For example, the art market has been accused of being an ideal vehicle for money laundering due to several unique aspects of art such as the subjective value of artworks as well as the secrecy of auction houses about the identity of the buyer and seller.
- Shell companies and trusts: Trusts and shell companies disguise the true owners of money. Trusts and corporate vehicles, depending on the jurisdiction, need not disclose their true owner. Sometimes referred to by the slang term *rathole*, though that term usually refers to a person acting as the fictitious owner rather than the business entity.
- Round-tripping: Here, money is deposited in a controlled foreign corporation offshore, preferably in a tax haven where minimal records are kept, and then shipped back as a foreign direct investment, exempt from taxation. A variant on this is to transfer money to a law firm or similar organization as funds on account of fees, then to cancel the retainer and, when the money is remitted, represent the sums received from the lawyers as a legacy under a will or proceeds of litigation.
- Bank capture: In this case, money launderers or criminals buy a controlling interest in a bank, preferably in a jurisdiction with weak money laundering controls, and then move money through the bank without scrutiny.
- Casinos: In this method, an individual walks into a casino and buys chips with illicit cash. The individual will then play for a relatively short time. When the person cashes in the chips, they will expect to take payment in a check, or at least get a receipt so they can claim the proceeds as gambling winnings.
- Other gambling: Money is spent on gambling, preferably on high odds games. One way to minimize risk with this method is to bet on every possible outcome of some event that has many possible outcomes, so no outcome(s) have

short odds, and the bettor will lose only the vigorish and will have one or more winning bets that can be shown as the source of money. The losing bets will remain hidden.

- Real estate: Someone purchases real estate with illegal proceeds and then sells the property. To outsiders, the proceeds from the sale look like legitimate income. Alternatively, the price of the property is manipulated: the seller agrees to a contract that underrepresents the value of the property, and receives criminal proceeds to make up the difference.
- Black salaries: A company may have unregistered employees without written contracts and pay them cash salaries. Dirty money might be used to pay them.
- Tax amnesties: For example, those that legalize unreported assets and cash in tax havens.
- Life insurance business: Assignment of policies to unidentified third parties and for which no plausible reasons can be ascertained.
- By using national banking services smurfing, Muiltiple tier of accounts,funnel accounts,Contra transactions,DD,cash depost and transfer fund connected accounts, front companies, legimate accounts, dormant accounts(Mostly used by terrorists) and wire transfer
- Using remittance ,prepaid cards, money changers,credit and debit cards

By using The credit card industry includes: case study

Credit card associations, such as American Express,MasterCard and Visa, which license member banks toissue bankcards, authorize merchants to accept thosecards, or bothIssuing banks, which solicit potential customers and issue the credit cards.Acquiring banks, which process transactions for merchants who accept credit cards.
Third-party processors, which contract with issuing or acquiring banks to provide transaction processing andother credit card–related services for the banks.Credit card accounts are not likely to be used in the initialplacement stage of money laundering because the industrygenerally restricts cash payments. They are more likely to be usedin the layering or integration stages.

Example
Money launderer Josh prepays his credit card using illicit funds that he has already introduced into thebanking system, creating a credit balance on his account. Josh then requests a credit refund, whichenables him to further obscure the origin of the funds, which constitutes layering. Josh then uses the illicitmoney he placed in his bank account and the creditcard refund to pay for a new kitchen that he bought.Through these steps he has integrated his illicit fundsinto the financial system.

- A money launderer could put ill-gotten funds in accounts at banksoffshore and then access these funds using credit and debitcards associated with the offshore account. Alternatively, he couldsmuggle the cash out of one country into an offshore jurisdictionwith lax regulatory oversight, place the cash in offshore banks and— again — access the illicit funds using credit or debit cards.In a 2002 Report called "Extent of Money Laundering throughCredit Cards Is Unknown," the U.S. Government AccountabilityOffice, the Congressional watchdog of the United States, offered hypothetical money laundering scenarios using credit cards. One
  example was: "[Money launderers establish a legitimate businessin the U.S. as a 'front' for their illicit activity. They establish a bank account with a U.S.-based bank and obtain credit cards and ATM cards under the name of the 'front business.' Funds from theirillicit activities are deposited into the bank account in the United States. While in another country, where their U.S.-based bank hasaffiliates, they make withdrawals from their U.S. bank account,using credit cards and ATM cards. Money is deposited by one of their cohorts in the U.S. and is transferred to pay off the credit cardloan or even prepay the credit card. The bank's online services make it possible to transfer funds between checking and creditcard accounts."

ML Global measures can be achieved by

A. Engagement of international organizations
B. UNO initiatives like Vienna convention in 1988, Political declaration in 1998 , The Palermo convention in 2003
C. International monetary fund
D. Financial intelligence units (In india 15th nov 2004 , Director EIU economic intelligence council, Headed by finance Minister)
E. Egmont group of FIUs..1995 (151 FIUs)

7. **FATF:**::

The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions. The objectives of the FATF are to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF is therefore a "policy-making body" which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

The FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a co-ordinated response to these threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations were revised in 1996, 2001, 2003 and most recently in 2012 to ensure that they remain up to date and relevant, and they are intended to be of universal application.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

The FATF's decision making body, the FATF Plenary, meets three times per year.

FATF HQ in Paris

FATF currently comprises 34 member jurisdictions and 12 regional organizations

FATF RECOMMENDATIONS. ::

Money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction are serious threats to security and the integrity of the financial system.

The FATF Standards have been revised to strengthen global safeguards and further protect the integrity of the financial system by providing governments with stronger tools to take action against financial crime. At the same time, these new standards will address new priority areas such as corruption and tax crimes.

The revision of the Recommendations aims at achieving a balance:

On the one hand, the requirements have been specifically strengthened in areas which are higher risk or where implementation could be enhanced. They have been expanded to deal with new threats such as the financing of proliferation of weapons of mass destruction, and to be clearer on transparency and tougher on corruption.
On the other, they are also better targeted – there is more flexibility for simplified measures to be applied in low risk areas. This risk-based approach will allow financial institutions and other designated sectors to apply their resources to higher risk areas.
The FATF Recommendations are the basis on which all countries should meet the shared objective of tackling money laundering, terrorist financing and the financing of proliferation. The FATF calls upon all countries to effectively implement these measures in their national systems.

FATF Recommendations 2012

A – AML/CFT POLICIES AND COORDINATION

1 - Assessing risks & applying a risk-based approach

2 - National cooperation and coordination

B – MONEY LAUNDERING AND CONFISCATION

3.Moneylaundering offence

4 - Confiscation and provisional measures

C – TERRORIST FINANCING AND FINANCING OF PROLIFERATION

5 - SRII Terrorist financing offence

6 - SRIII Targeted financial sanctions related to terrorism & terrorist financing

7 - Targeted financial sanctions related to proliferation

8 - Non-profit organisations

D – PREVENTIVE MEASURES
9 - Financial institution secrecy laws

Customer due diligence and record keeping

10 - Customer due diligence
11 - Record keeping

Additional measures for specific customers and activities

12 - Politically exposed persons
13 - Correspondent banking
14 - Money or value transfer services
15 - New technologies
16 - Wire transfers

Reliance, Controls and Financial Groups

17 - Reliance on third parties
18 - Internal controls and foreign branches and subsidiaries
19 - Higher-risk countries

Reporting of suspicious transactions

20 - Reporting of suspicious transactions
21 - Tipping-off and confidentiality

Designated non-financial Businesses and Professions (DNFBPs)

22 - DNFBPs: Customer due diligence
23 - DNFBPs: Other measures

E – TRANSPARENCY AND BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND ARRANGEMENTS
24 - Transparency and beneficial ownership of legal persons
25 - Transparency and beneficial ownership of legal arrangements

F – POWERS AND RESPONSIBILITIES OF COMPETENT AUTHORITIES AND OTHER INSTITUTIONAL MEASURES
Regulation and Supervision

26 - Regulation and supervision of financial institutions
27 - Powers of supervisors
28 - Regulation and supervision of DNFBPs

Operational and Law Enforcement

29 - Financial intelligence units
30 - Responsibilities of law enforcement and investigative authorities
31 - Powers of law enforcement and investigative authorities
32 - Cash couriers

General Requirements

33 - Statistics
34 - Guidance and feedback

Sanctions

35 - Sanctions

G – INTERNATIONAL COOPERATION
36 - International instruments
37 - Mutual legal assistance
38 - Mutual legal assistance: freezing and confiscation
39 - Extradition
40 - Other forms of international cooperation

8.FATF IX Special Recommendations on Terrorist Financing:::

Recognising the vital importance of taking action to combat the financing of terrorism, the FATF has agreed these Recommendations, which, when combined with the FATF Forty Recommendations on money laundering, set out the basic framework to detect, prevent and suppress the financing of terrorism and terrorist acts.

I. Ratification and implementation of UN instruments Each country should take immediate steps to ratify and to implement fully the 1999 United Nations
International Convention for the Suppression of the Financing of Terrorism.
Countries should also immediately implement the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts, particularly United Nations Security Council Resolution 1373.

II. Criminalising the financing of terrorism and associated money laundering
Each country should criminalise the financing of terrorism, terrorist acts and terrorist organisations. Countries should ensure that such offences are designated as money laundering predicate offences.

III. Freezing and confiscating terrorist assets Each country should implement measures to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with the United Nations resolutions relating to the prevention and suppression of the financing of terrorist acts. Each country should also adopt and implement measures, including legislative ones, which would enable the competent authorities to seize and confiscate property that is the proceeds of, or used in, or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations.

IV. Reporting suspicious transactions related to terrorism If financial institutions, or other businesses or entities subject to anti-money laundering obligations, suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organisations, they should be required to report promptly their suspicions to the competent authorities.

V. International Co-operation Each country should afford another country, on the basis of a treaty, arrangement or other mechanism for mutual legal assistance or information exchange, the greatest possible measure of assistance in connection with criminal, civil enforcement, and administrative investigations, inquiries and proceedings relating to the financing of terrorism, terrorist acts and terrorist organisations.
Countries should also take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, terrorist acts or terrorist organisations, and should have procedures in place to extradite, where possible, such individuals.
VI. Alternative Remittance Each country should take measures to ensure that persons or legal entities, including agents, that provide a service for the transmission of money or value, including transmission through an informal money or value transfer system or network, should be licensed or registered and subject to all the FATF Recommendations that apply to banks and non-bank financial institutions. Each country should ensure that persons or legal entities that carry out this service illegally are subject to administrative, civil or criminal sanctions.

VII. Wire transfers Countries should take measures to require financial institutions, including money remitters, to include accurate and meaningful originator information (name, address and account number) on funds transfers and related messages that are sent, and the information should remain with the transfer or
related message through the payment chain. Countries should take measures to ensure that financial institutions, including money remitters, conduct enhanced scrutiny of and monitor for suspicious activity funds transfers which do not contain complete originator information (name, address and account number).

VIII. Non-profit organi sations Countries should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism. Non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused:

(i) by terrorist organisations posing as legitimate entities;

(ii) to exploit legitimate entities as conduits for terrorist financing, including for the purpose of escaping asset freezing measures; and (iii) to conceal or obscure the clandestine diversion of funds intended for legitimate purposes to terrorist organisations. IX. Cash Couriers Countries should have measures in place to detect the physical cross-border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation. Countries should ensure that their competent authorities have the legal authority to stop or restrain currency or bearer negotiable instruments that are suspected to be related to terrorist financing or money laundering, or that are falsely declared or disclosed. Countries should ensure that effective, proportionate and dissuasive sanctions are available to deal with persons who make false declaration(s) or disclosure(s). In cases where the currency or bearer negotiable instruments are related to terrorist financing or money laundering, countries should also adopt measures, including legislative ones consistent with Recommendation 3 and Special Recommendation III, which would enable the confiscation of such currency or instruments.

9.FATF Regional bodies

There are eight regional FATF-style bodies and FATF Associate Members that have similar form and functions to those of FATF. Many FATF member countries are also members of these bodies.

Asia/Pacific Group on Money Laundering (APG).

Caribbean Financial Action Task Force (CFATF).

Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) (formerly PC-R-EV).

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG).

Eurasian Group (EAG).

Financial Action Task Force of South America against Money Laundering (GAFISUD – Grupo de Acción Financiera de Sudamérica)

Intergovernmental Action Group against Money-Laundering in West Africa (GIABA – Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Quest)

Middle East and North Africa Financial Action Task Force (MENAFATF)

10. **cuckoo smurfing.::**

In 2005, FATF added a new term to the vast money laundering lexicon – "cuckoo smurfing.

The term, mentioned in the organization's 2005 Typologies Report,refers to a form of money laundering linked to alternativeremittance systems, in which criminal funds are transferred through the accounts of unwitting persons who are expecting genuinefunds or payments from overseas. The term cuckoo smurfing firstoriginated in investigations in the United Kingdom, where it is asignificant money laundering technique.The cuckoo is a European bird that is a parasite because it laysits eggs in the nests of other birds, which hatch them and rearthe offspring. The main difference between traditional structurerand cuckoo smurfing is that in the latter the third parties who holdthe bank accounts being used are not aware of the fact that illicitmoney is being deposited into their accounts.Cuckoo smurfing requires the work of an insider within a financialinstitution and is generally a four step process:

The first step occurs when a customer provides fundsto an alternative remitter for transfer to a beneficiary,generally in another country.

The next step involves the insider, who will provide the transaction details (beneficiary name, bank, accountnumber and amount) of the transfer to an associatein the foreign country where the beneficiary of thetransfer is located. The associate in the foreign countrywill have cash that needs to be placed into the financialsystem.

The associate in the foreign country will then depositcash into the bank account of the intended beneficiary.The beneficiary will receive the full amount of thetransfer and the associate in the foreign country will be able to place some of its cash into the financial system

The associate in the foreign country then arranges to get the funds from the alternate remitter, using oneof the methods by which alternate remitters transferfunds. In this case, the associate in the foreign countrywill have laundered the funds and will have legitimate funds to replace the criminally derived ones depositedinto the beneficiary's account.

11. Wolfsberg Group:: 13 Banks

Banco Santander
Bank of America
Bank of Tokyo-Mitsubishi UFJ
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
J.P. Morgan Chase
Société Générale
Standard Chartered Bank
UBS

The Wolfsberg Group is an association of 13 global banks that aims to develop financial services industry standards and related products for Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policiesThe Group first came together in 2000 at the Wolfsberg castle in Switzerland, accompanied by representatives of Transparency International, to draft anti-money laundering guidelines for private banking that, when implemented, would mark an unprecedented private-sector assault on the laundering of corruption proceeds. Their principles hold no force of law and carry no penalties for those who do not abide by them. The Wolfsberg Anti-Money Laundering Principles for Private Banking was published in October 2000 and was revised in May 2002. These principles recommend controls for private banking that range from the basic, such as customer identification, to enhanced due diligence, such as heightened scrutiny of individuals who "have or have had positions of public trust." The banks that released the principles with Transparency International said that the principles would "make it harder for corrupt people to deposit their ill-gotten gains in the world's banking system." The principles say banks will "endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate." They highlight the need to identify the beneficial owner of funds "for all accounts" when that person is someone other than the client, and urge private bankers to perform due diligence on "money managers and similar intermediaries" to determine that the middlemen have a "satisfactory" due diligence process for their clients or a regulatory obligation to conduct such due diligence. The principles recommend that "at least one person other than the private banker" should approve all new clients and accounts.

The principles list several situations that require further due diligence, including activities that involve:

Public officials, including individuals holding, or having held, positions of public trust, as well as their families and close associates. High-risk countries, including countries "identified by credible sources as having inadequate anti-moneylaundering standards or representing high-risk for crime and corruption." High-risk activities, involving clients and beneficial owners whose source of wealth "emanates from activities known to be susceptible to money laundering." The Wolfsberg principles say that banks should have written policies on the "identification of and follow-up on unusual or suspicious activities," and should include a definition of what is suspicious, as well as examples of such activity. They recommend a "sufficient" monitoring system that uses the private banker's knowledge of the types of activity that would be suspicious for particular clients. They also outline mechanisms that can be used to identify suspicious activity, including meetings, discussions and in-country visits with clients and steps that should be taken when suspicious activity is detected. The principles also address: Reporting to manageMent of money laundering issues. AML training. Retention of relevant documents. Deviations from policy. Creation of an anti-money laundering department and an AML policy.

In May 2002, the Wolfsberg Principles for Private Banking were revised. A section was added prohibiting the use of internal non-client accounts (sometimes referred to as "concentration" accounts) to keep clients from being linked to the movement of funds on their behalf (i.e., banks should forbid the use of such internal accounts in a manner that would prevent officials from appropriately monitoring movements of client funds). The Wolfsberg Group also issued guidelines in early 2002 on "The Suppression of the Financing of Terrorism," outlining the roles of financial institutions in the fight against money laundering and terrorism financing. The Wolfsberg recommendations include:
Providing official lists of suspected terrorists on a globally coordinated basis by relevant authorities.
Including adequate information in the lists to help institutions search customer databases efficiently.
Providing prompt feedback to institutions following circulation of the official lists. Providing information on the manner, means and methods used by terrorists. Developing government guidelines for business sectors and activities identified as high-risk for terrorism financing. Developing uniform global formats for funds transfers that assist in the detection of terrorism financing. The group also recommends that financial institutions be protected by a safe harbor immunity to encourage them to share information and to report to authorities. The Wolfsberg Group also committed itself to recommending enhanced due diligence for "business relationships with remittance businesses, exchange houses, casas de cambio, bureaux de change and money transfer agents…" and committed its members to taking enhanced due diligence steps for high-risk customers or those in high-risk sectors, and activities "such as underground banking businesses or alternative remittance systems." In 2002, Wolfsberg issued guidelines on "Anti-Money Laundering Principles for Correspondent Banking" that outlined steps financial institutions should take to combat money laundering and terrorism financing through correspondent banking

12.AML/CFT legislation in Major countries
A. EUROPE a) European convention on the suppression of terrorism 1977 b)EC on laundering ,search , Seizure from crime 1993 B.US a) Bank secrecy act 1970 b)Money laundering control Act 1986 c) Anti drug abuse act 1988 d)Annuzio –Wylie AML act 1992 d)ML Suppression Act 1994 f)ML and Financial crimes strategy act 1998 G) USA PETRIOT ACT 2001

C. UK

. Terrorism Act 2000

- Anti-terrorism, Crime and Security Act 2001
- Proceeds of Crime Act 2002
- Serious Organised Crime and Police Act 2005
- Money Laundering Regulations 2007
- Money Laundering Regulation, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
- Sanctions and Anti-Money Laundering Act 2018

13.AML/CFT IN INDIA

In 2002, the Parliament of India passed an act called the Prevention of Money Laundering Act, 2002. The main objectives of this act are to prevent money-laundering as well as to provide for confiscation of property either derived from or involved in, money-laundering.

Section 12 (1) describes the obligations that banks, other financial institutions, and intermediaries have to

a. Maintain records that detail the nature and value of transactions, whether such transactions comprise a single transaction or a series of connected transactions, and where these transactions take place within a month.
b. Furnish information on transactions referred to in clause (a) to the Director within the time prescribed, including records of the identity of all its clients.

    a. Section 12 (2) prescribes that the records referred to in sub-section (1) as mentioned above, must be maintained for ten years after the transactions finished. It is handled by the Indian Income Tax Department.

b. The provisions of the Act are frequently reviewed and various amendments have been passed from time to time.[

c. Most money laundering activities in India are through political parties, corporate companies and the shares market. These are investigated by the Enforcement Directorate and Indian Income Tax Department.[According to Government of India, out of the total tax arrears of ₹2,480 billion (US$37 billion) about ₹1,300 billion (US$19 billion) pertain to money laundering and securities scam cases.

d. Bank accountants must record all transactions over Rs. 1 million and maintain such records for 10 years. Banks must also make cash transaction reports (CTRs) and suspicious transaction reports over Rs. 1 million within 7 days of initial suspicion. They must submit their reports to the Enforcement Directorate and Income Tax Department.[

14**.THE PREVENTION OF MONEY LAUNDERING ACT**

The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. PMLA and the Rules notified there under came into force with effect from July 1, 2005 . Director, FIU-IND and Director (Enforcement) have been conferred with exclusive and concurrent powers under relevant sections of the Act to implement the provisions of the Act.

The PMLA and rules notified thereunder impose obligation on banking companies, financial institutions and intermediaries to verify identity of clients, maintain records and furnish information to FIU-IND. PMLA defines money laundering offence and provides for the freezing, seizure and confiscation of the proceeds of crime.

PMLA 2002 Overview::

Section 1 - Short title, extent and commencement
Section 2 - Definitions
Section 3 - Offence of Money-Laundering
Section 4 - Punishment for Money Laundering
Section 12 - Obligations-Reporting Entity to maintain records
Section 12A - Obligations-Access to information
Section 13 - Powers of the Director
Section 14 - No civil proceedings
Section 15 - Powers to prescribe procedure
Section 26 - Appellate Tribunal
Section 39 - Right of Appellant
Section 40 - Deemed to be Public Servants
Section 41 - Restriction on Civil Courts
Section 42 - Appeal to High Court
Section 44 - Offences triable by Special Courts
Section 48 - Authorities under the Act
Section 49 - Appointment of Authorities and Other Officers
Section 50 - Summons, production of documents etc.
Section 54 - Other authorities empowered and required to assist
Section 56 - Agreements with foreign countries
Section 66 - Disclosure of information
Section 69 - Recovery of fines
Section 75 - Power to remove difficulties

15.FIU –IND

Overview of FIU-IND

Financial Intelligence Unit – India (FIU-IND) was set by the Government of India vide O.M. dated 18th November 2004 as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

Functions of FIU-IND::

The main function of FIU-IND is to receive cash/suspicious transaction reports, analyse them and, as appropriate, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities . The functions of FIU-IND are: Collection of Information: Act as the central reception point for receiving Cash Transaction reports (CTRs), Cross Border Wire Transfer Reports (CBWTRs), Reports on Purchase or Sale of Immovable Property (IPRs) and Suspicious Transaction Reports (STRs) from various reporting entities.

Analysis of Information: Analyze received information in order to uncover patterns of transactions suggesting suspicion of money laundering and related crimes.

Sharing of Information:Share information with national intelligence/law enforcement agencies, national regulatory authorities and foreign Financial Intelligence Units. Act as Central Repository:Establish and maintain national data base on cash transactions and suspicious transactions on the basis of reports received from reporting entities.

Coordination:Coordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes.

Research and Analysis:Monitor and identify strategic key areas on money laundering trends, typologies and developments.

Organization Strength of FIU-IND

FIU-IND is a multi disciplinary body with a sanctioned strength of 74 personnel. These are being inducted from different organizations namely Central Board of Direct Taxes (CBDT), Central Board of Excise and Customs (CBEC), Reserve Bank of India (RBI), Securities Exchange Board of India (SEBI), Department of Legal Affairs and Intelligence agencies

Organizational structure

Financial Intelligence Unit – India (FIU-IND)

Financial Intelligence Unit – India (FIU-IND) was set by the Government of India in 2004 as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

Functions of FIU-IND

The main function of FIU-IND is to receive cash/suspicious transaction reports, analyse them and, as appropriate, disseminate valuable financial information to intelligence/enforcement agencies and regulatory authorities . The functions of FIU-IND are:

Collection of Information: Act as the central reception point for receiving Cash Transaction reports (CTRs) and Suspicious Transaction Reports (STRs) from various reporting entities.

Analysis of Information: Analyze received information in order to uncover patterns of transactions suggesting suspicion of money laundering and related crimes.

Sharing of Information: Share information with national intelligence/law enforcement agencies, national regulatory authorities and foreign Financial Intelligence Units.

Act as Central Repository: Establish and maintain national data base on cash transactions and suspicious transactions on the basis of reports received from reporting entities.

Coordination: Coordinate and strengthen collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes.

Research and Analysis: Monitor and identify strategic key areas on money laundering trends, typologies and developments.

Organisational Set-up

FIU-IND is a multi disciplinary body headed by a Director. Personnel in this Unit are being inducted from different organizations namely Central Board of Direct Taxes (CBDT), Central Board of Excise and Customs (CBEC), Reserve Bank of India (RBI), Securities Exchange Board of India (SEBI), Department of Legal Affairs and Intelligence agencies.

Authorities at FIU-IND

According to Section 48 of the Prevention of Money Laundering Act, 2002 there shall be the following classes of authorities for the purposes of this Act, namely:-
(a) Director or Additional Director or Joint Director,
(b) Deputy Director,
(c) Assistant Director, and
(d) such other class of officers as may be appointed for the purposes of this Act.

Appointment of Authorities

As per Section 49 of the Prevention of Money Laundering Act, 2002:
(1) The Central Government may appoint such persons as it thinks fit to be authorities for the purposes of this Act.
(2) Without prejudice to the provisions of sub-section (1), the Central Government may authorise the Director or an Additional Director or a Joint Director or a Deputy Director or an Assistant Director appointed under that sub-section to appoint other authorities below the rank of an Assistant Director.
(3) Subject to such conditions and limitations as the Central Government may impose, an authority may exercise the powers and discharge the duties conferred or imposed on it under this Act.
Director and officers subordinate to him deemed to be public servants Section 40 of the Prevention of Money Laundering Act, 2002 declares the Chairperson, Members and other officers and employees of the Appellate Tribunal, the Adjudicating Authority, Director and the officers subordinate to him shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code, 1860 (45 of 1860).

Powers of the Director

Section 13 of the Prevention of Money Laundering Act, 2002 confers following powers on the Director to ensure compliance:
(1) The Director may, either of his own motion or on an application made by any authority, officer or person, call for records referred to in sub-section (1) of section 12 and may make such inquiry or cause such inquiry to be made, as he thinks fit.
(2) If the Director, in the course of any inquiry, finds that a banking company, financial institution or an intermediary or any of its officers has failed to comply with the provisions contained in section 12, then, without prejudice to any other action that may be taken under any other provisions of this Act, he may, by an order, levy a fine on such banking company
or financial institution or intermediary which shall not be less than ten thousand rupees but may extend to one lakh rupees for each failure.
(3) The Director shall forward a copy of the order passed under sub-section (2) to every banking company, financial institution or intermediary or person who is a party to the proceedings under that sub-section. Powers of authorities regarding summons, production of documents and to give evidence: Section 50 of the Prevention of Money Laundering Act, 2002 confers following powers of summons, production of documents and to give evidence etc.:
(1) The Director shall, for the purposes of section 13, have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a suit in respect of the following matters, namely:-
(a) discovery and inspection;
(b) enforcing the attendance of any person, including any officer of a banking company,
financial institution or a company, and examining him on oath;
(c) compelling the production of records;
(d) receiving evidence on affidavits;
(e) issuing commissions for examination of witnesses and documents; and
(f) any other matter which may be prescribed
(2) The Director, Additional Director, Joint Director, Deputy Director or Assistant Director shall have power to summon any person whose attendance he considers necessary whether to give evidence or to produce any records during the course of any investigation or proceeding under this Act.
(3) All the persons so summoned shall be bound to attend in person or through authorized agents, as such officer may direct, and shall be bound to state the truth upon any subject which they are examined or make statements, and produce such documents as may be required.
(4) Every proceeding under sub-sections (2) and (3) shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228 of the Indian Penal Code, 1860 (45 of 1860).
(5) Subject to any rules made in this behalf by the Central Government, any officer referred to in sub-section (2) may impound and retain in his custody for such period, as he thinks fit, any records produced before him in any proceedings under this Act:
Provided that an Assistant Director or a Deputy Director shall not -
(a) impound any records without recording his reasons for so doing; or
(b) retain in his custody any such records for a period exceeding three months, without obtaining the prior approval of the Director. Assistance from other authorities for enforcement of the Act Section 54 of the Prevention of Money Laundering Act, 2002 empowers and requires various authorities to assist in the enforcement of the act. The following officers are empowered and required to assist the authorities in the enforcement of this Act, namely:-

(a) officers of the Customs and Central Excise Departments;
(b) officers appointed under sub-section (1) of section 5 of the Narcotic Drugs and
Psychotropic Substances Act, 1985 (61 of 1985);
(c) income-tax authorities under sub-section (1) of section 117 of the Income-tax Act, 1961 (43 of 1961);
(d) officers of the stock exchange recognised under section 4 of the Securities Contracts (Regulation) Act, 1956 (42 of 1956);
(e) officers of the Reserve Bank of India constituted under sub-section (1) of section 3 of the Reserve Bank of India Act, 1934 (2 of 1934);
(f) officers of Police;
(g) officers of enforcement appointed under sub-section (1) of section 36 of the Foreign Exchange Management Act, 1973 (40 of 1999);
(h) officers of the Securities and Exchange Board of India established under section 3 of the Securities and Exchange Board of India Act, 1992 (15 of 1992);
(i) officers of any other body corporate constituted or established under a Central Act or a State Act;
(j) such other officers of the Central Government, State Government, local authorities or banking companies as the Central Government may, by notification, specify, in this behalf.
Agreements with foreign countries
Section 56 of the Prevention of Money Laundering Act, 2002 provides for agreements with foreign countries to facilitate exchange of information with them:
(1) The Central Government may enter into an agreement with the Government of any country outside India for-
(a) enforcing the provisions of this Act;
(b) exchange of information for the prevention of any offence under this Act or under the
corresponding law in force in that country or investigation of cases relating to any offence under this Act. and may, by notification in the Official Gazette, make such provisions as may be necessary for implementing the agreement.
(2) The Central Government may, by notification in the Official Gazette, direct that the application of this Chapter in relation to a contracting State with which reciprocal arrangements have been made, shall be subject to such conditions, exceptions or qualifications as are specified in the said notification.

Disclosure of information

Section 66 of the Prevention of Money Laundering Act, 2002 provides for disclosure of information to other officers, authority or body:
The Director or any other authority specified by him by a general or special order in this behalf may furnish or cause to be furnished to-
(i) any officer, authority or body performing any functions under any law relating to imposition of any tax, duty or cess or to dealings in foreign exchange, or prevention of illicit traffic in the narcotic drugs and psychotropic substances under the Narcotic Drugs and Psychotropic Substances Act, 1985 (61 of 1985); or
(ii) such other officer, authority or body performing functions under any other law as the Central Government may, if in its opinion it is necessary so to do in the public interest, specify by notification in the Official Gazette in this behalf, any information received or obtained by such Director or any other authority, specified by him in the performance of their functions under this Act, as may, in the opinion of the Director or the other authority so specified by him, be necessary for the purpose of the officer, authority or body specified in clause (i) or clause (ii) to perform his or its functions under that law.

Recovery of fines

Section 69 of the Prevention of Money Laundering Act, 2002 refers to recovery of fines. Where any fine imposed on any person under section 13 or section 63 is not paid within six months from the day of imposition of fine, the Director or any other officer authorised by him in this behalf may proceed to recover the amount from the said person in the same manner as prescribed in Schedule 11 of the Income-tax Act, 1961 (43 of 1961) for the recovery of arrears and he or any officer authorised by him in this behalf shall have all the powers of the Tax Recovery Officer mentioned in the said Schedule for the said purpose. The new network, called FINnet (Financial Intelligence Network), is a technology-based secure platform for bringing together investigative and enforcement agencies to collect, analyse and disseminate valuable financial information for combating money laundering and related crimes.

Restriction on Civil Court Jurisdiction

Section 41 of the Prevention of Money Laundering Act, 2002 says that no civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Director, an Adjudicating Authority or the Appellate Tribunal is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act."
Appeal to Appellate Tribunal Section 26 of the Prevention of Money Laundering Act, 2002 deals with appeal to Appellate Tribunal.
(1) Save as otherwise provided in sub-section (3), the Director or any person aggrieved by an order made by the Adjudicating Authority under this Act, may prefer an appeal to the Appellate Tribunal.
(2) Any banking company, financial institution or intermediary aggrieved by any order of the Director made under sub-section (2) of section 13, may prefer an appeal to the Appellate Tribunal.

(3) Every appeal preferred under sub-section (1) or sub-section (2) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Adjudicating Authority or Director is received and it shall be in such form and be accompanied by such fee as may be prescribed:
Provided that the Appellate Tribunal may, after giving an opportunity of being heard, entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.
(4) On receipt of an appeal under sub-section (1), or sub-section (2), the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.
(5) The Appellate Tribunal shall send a copy of every order made

Right of Appellant
Section 39 of the Prevention of Money Laundering Act, 2002 provides for the right of the appellant.
(1) A person preferring an appeal to the Appellate Tribunal under this Act may either appear in person or take the assistance of an authorised representative of his choice to present his case before the Appellate Tribunal.
Explanation - For the purposes of this sub-section, the expression "authorized representative" shall have the same meaning as assigned to it under sub-section (2) of section 288 of the Income Tax Act, 1961.
(2) The Central Government or the Director may authorise one or more authorized representatives or any of its officers to act as presenting officers and every person so authorised may present the case with respect to any appeal before the Appellate Tribunal.
Appeal to High Court
Section 42 of the Prevention of Money Laundering Act, 2002 provides for appeal to High Court:
"Any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Appellate Tribunal to him on any question of law or fact arising out of such order: Provided that the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.
Explanation.-For the purposes of this section, "High Court" means-
(i) the High Court within the jurisdiction of which the aggrieved party ordinarily resides or carries on business or personally works for gain; and
(ii) where the Central Government is the aggrieved party, the High Court within the jurisdiction of which the respondent, or in a case where there are more than one respondent, any of the respondents, ordinarily resides or carries on business or personally works for gain.
Offences which can be seen by Special Courts
Section 44 of the Prevention of Money Laundering Act, 2002 provides for trial by Special Courts:
(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974),-
a. the schedule offence and the offence punishable under section 4 shall be tried only by the Special Court constituted for the area in which the offence has been committed; Provided that the Special Court , trying a schedule offence before the commencement of this Act, shall continue to try such scheduled offence, or
b. a Special Court may, upon a complaint made by an authority authorised in this behalf under this Act take cognizance of the offence for which the accused is committed to it for trial.
(2) Nothing contained in this section shall be deemed to affect the special powers of the High Court regarding bail under section 439 of the Code of Criminal Procedure, 1973 (2 of 1974) and the High Court may exercise such powers including the power under clause (b) of sub-section (1) of that section as if the reference to "Magistrate" in that section includes also a reference to a "Special Court" designated under section 43.

KYC SHORT NOTES:

1. The objective of KYC/AML/CFT guidelines is to prevent banks/FIs from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities.
2. The PMLA came into effect from 1st July 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on 1st July, 2005 by the Department of Revenue, Ministry of Finance, Government of India. The PMLA has been further amended vide notification dated March 6, 2009 and inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as prescribed in Section 12 A read with Section 24 of the Securities and Exchange Board of India Act, 1992 (SEBI Act) will now be treated as a scheduled offence under schedule B of the PMLA.

3. KYC procedures also enable banks/FIs to know/understand their customers and their financial dealings better and manage their risks prudently.
4. For the purpose of KYC Norms, a 'Customer' is defined as a person who is engaged in a financial transaction or activity with a reporting entity and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.
5. "Designated Director" means a person designated by the reporting entity (bank, financial institution, etc.) to ensure overall compliance with the obligations imposed under chapter IV of the PML Act.
6. **In terms of PML Act a 'person' includes**: (i) an individual, (ii) a Hindu undivided family, (iii) a company, (iv) a firm, (v) an association of persons or a body of individuals, whether incorporated or not, (vi) every artificial juridical person, not falling within any one of the above persons (i to v), and (vii) any agency, office or branch owned or controlled by any of the above persons (i to vi).
7. "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes- (i) opening of an account; (ii) deposits, withdrawal, exchange or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means; (iii) the use of a safety deposit box or any other form of safe deposit; (iv) entering into any fiduciary relationship; (v) any payment made or received in whole or in part of any contractual or other legal obligation; or (vi) establishing or creating a legal person or legal arrangement.
8. **Banks/FIs should frame their KYC policies incorporating the following four key elements:** (i) Customer Acceptance Policy (CAP); (ii) Customer Identification Procedures (CIP); (iii) Monitoring of Transactions; and (iv) Risk Management.
9. Documents and other information to be collected from different categories of customers depending on perceived risk and the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time.
10. **Customer Identification Procedure (CIP) :** Customer identification means undertaking client due diligence measures while commencing an account-based relationship including identifying and verifying the customer and the beneficial owner on the basis of one of the OVDs
11. Customer Due Diligence requirements (CDD) while opening accounts
12. introduction is not necessary for opening of accounts under PML Act and Rules or the Reserve Bank's extant instructions, banks/FIs should not insist on introduction for opening of bank accounts

1. **Small Accounts** If an individual customer does not possess either any of the OVDs or the documents applicable in respect of simplified procedure (as detailed at paragraph 2.3 above), 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 rupees one lakh; the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand and the balance at any point of time does not exceed rupees fifty thousand. A 'small account' maybe opened on the basis of a self-attested photograph and affixation of signature or thumb print.
2. 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;
3. 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.
4. Where a customer categorised as low risk expresses inability to complete the documentation requirements on account of any reason that the bank considers to be genuine, and where it is essential not to interrupt the normal conduct of business, the bank may complete the verification of identity within a period of six months from the date of establishment of the relationship.
5. Procedure to be followed in respect of foreign students : Banks should follow the following procedure for foreign students studying in India: 1) Banks may open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with visa & immigration endorsement) bearing the proof of identity and address in the home country together with a photograph and a letter offering admission from the educational institution in India. 2) Banks should obtain a declaration about the local address within a period of 30 days of opening the account and verify the said local address. 3) During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 or equivalent into the account and a cap of

monthly withdrawal to Rs. 50,000/-, pending verification of address. 4) The account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account. Students with Pakistani and Bangladesh nationality will need prior approval of the Reserve Bank for opening the account.

Where the customer is a company, one certified copy each of the following documents are required for customer identification: (a) Certificate of incorporation; (b) Memorandum and Articles of Association; (c) A resolution from the Board of Directors and power of attorney granted to its managers, officers or employees to transact on its behalf and (d) An officially valid document in respect of managers, officers or employees holding an attorney to transact on its behalf

13. Where the customer is a partnership firm, one certified copy of the following documents is required for customer identification: (a) registration certificate; (b) partnership deed and (c) an officially valid document in respect of the person holding an attorney to transact on its behalf.

14. Where the customer is a trust, one certified copy of the following documents is required for customer identification: (a) registration certificate; (b) trust deed and (c) an officially valid document in respect of the person holding a power of attorney to transact on its behalf.
15. Where the customer is an unincorporated association or a body of individuals, one certified copy of the following documents is required for customer identification: (a) resolution of the managing body of such association or body of individuals; (b) power of attorney granted 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/FI to collectively establish the legal existence of such an association or body of individuals.
16. **Proprietary concerns:** (1) For proprietary concerns, in addition to the OVD applicable to the individual (proprietor), any two of the following documents in the name of the proprietary concern are required to be submitted: (a) Registration certificate (b) Certificate/licence issued by the municipal authorities under Shop and Establishment Act. (c) Sales and income tax returns. (d) CST/VAT certificate. (e) Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities. (f) Licence/certificate of practice issued in the name of the proprietary concern by any professional body incorporated under a statute. (g) Complete Income Tax Return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected, duly authenticated/acknowledged by the Income Tax authorities. (h) Utility bills such as electricity, water, and landline telephone bills.
17. When the client accounts are opened by professional intermediaries: When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks, however, should not open accounts of such professional intermediaries who are bound by any client confidentiality that prohibits disclosure of the client details to the banks.
18. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look into the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is a regulated and supervised entity and has adequate systems in place to comply with the KYC requirements of the customers. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.
19. **Beneficial ownership** :When a bank/FI identifies a customer for opening an account, it should identify the beneficial owner(s) and take all reasonable steps in terms of Rule 9(3) of the PML Rules to verify his identity, as per guidelines provided below:

    (a) Where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have a controlling ownership interest or who exercises control through other meansExplanation- For the purpose of this sub-clause- 1. "Controlling ownership interest"

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

(b) Where the client is a partnership firm, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of capital or profits of the partnership.
(c) Where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has/have ownership of/entitlement to more than 15 per cent of the property or capital or profits of the unincorporated association or body of individuals.
(d) Where no natural person is identified under (a), (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official.
(e) Where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with 15% or more interest in the trust and any other natural person. exercising ultimate effective control over the trust through a chain of control or ownership.
(f) Where the client or the owner of the controlling interest is a company listed on a stock exchange, or is a subsidiary of such a company, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such companies.

20. KYC exercise should 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. Such KYC exercise may include all measures for confirming the identity and address and other particulars of the customer that the bank/FI may consider reasonable and necessary based on the risk profile of the customer, taking into account whether and when client due diligence measures were last undertaken and the adequacy of data obtained.

21. Freezing and closure of accounts :

(i) In case of non-compliance of KYC requirements by the customers despite repeated reminders by banks/FIs, banks/FIs may impose 'partial freezing' on such KYC non-compliant accounts in a phased manner.
(ai)During the course of such partial freezing, the account holders can revive their accounts by submitting the KYC documents as per instructions in force.
(bi) While imposing 'partial freezing', banks/FIs have to ensure that the option of 'partial freezing' is exercised after giving due notice of three months initially to the customers to comply with KYC requirements to be followed by a reminder giving a further period of three months.
(v) (iv) Thereafter, banks/FIs may impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts If the accounts are still KYC non-compliant after six months of imposing initial 'partial freezing' banks/FIs should disallow all debits and credits from/to the accounts thereby, rendering them inoperative.
(vi) Further, it would always be open to the bank/FI to close the account of such customers after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions, however, need to be taken at a reasonably senior level. In the circumstances when a bank/FI believes that it would no longer be satisfied about the true identity of the account holder, the bank/FI should file a Suspicious Transaction Report (STR) with Financial Intelligence Unit – India (FIU-IND) under Department of Revenue, Ministry of Finance, Government of India.

22. **At-par cheque facility availed by co-operative banks** : Some commercial banks have arrangements with co-operative banks under which the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for effecting their remittances and payments. Since theb'at par' cheque facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangement, banks should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising there from. For this purpose, banks 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.

23. In this regard, Urban Cooperative Banks (UCBs) are advised to utilize the 'at par' cheque facility only for the following purposes:
    (i) For their own use.
    (ii) For their account holders who are KYC complaint provided that all transactions of Rs.50,000/- or more should be strictly by debit to the customer's account.
    (iii) For walk-in customers against cash for less than Rs.50,000/- per individual. In order to utilise the 'at par' cheque facility in the above manner, UCBs should maintain the following:
    (i) Records pertaining to issuance of 'at par' cheques covering inter alia applicant's name and account number, beneficiary's details and date of issuance of the 'at par' cheque

    . (ii)Sufficient balances/drawing arrangements with the commercial bank extending such facility for purpose of honouring such instruments. UCBs should also ensure that all 'at par' cheques issued by them are crossed 'account payee' irrespective of the amount involved.
30. Simplified norms for Self Help Groups (SHGs) : KYC verification of all the members of SHG need not be done while opening the savings bank account of the SHG and KYC verification of all the office bearers would suffice. As regards KYC verification at the time of credit linking of SHGs, no separate KYC verification of the members or office bearers is necessary
31. **Walk-in Customer :** 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 Rs. 50,000/-, whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified. If a bank has reason to believe that a customer is intentionally structuring a transaction into a series of transactions below the threshold of Rs.50,000/- the bank should verify the identity and address of the customer and also consider filing a Suspicious Transactions Report (STR) to Financial Intelligence Unit – India (FIU-IND). In terms of Clause (b) (ii) of sub-Rule (1) of Rule 9 of the PML Rules, 2005 banks and financial institutions are required to verify the identity of the customers for all international money transfer operations.
32. **Issue of Demand Drafts, etc, for more than Rs.50,000/- :** Banks should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rs.50,000/- and above is effected by debit to the customer's account or against cheques and not against cash payment. Banks should not make payment of cheques/drafts/pay orders/banker's cheques if they are presented beyond the period of three months from the date of such instrument.
33. **Unique Customer Identification Code :** A Unique Customer Identification Code (UCIC) will help banks to identify the customers, avoid multiple identities, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. Banks have been advised to allot UCIC while entering into new relationships with individual customers as also the existing customers.
34. Banks/FIs should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of not less than once in six months.
35. Banks should closely monitor the transactions in accounts of marketing firms, especially accounts of Multi-level Marketing (MLM) Companies. Banks should analyse data 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. Where such features are noticed by the bank and in case they find such unusual operations in their accounts, the matter should be immediately reported to Reserve Bank and other appropriate authorities such as FIU-IND.
36. Banks/FIs 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 about the clients, their business and risk profile and where necessary, the source of funds.
37. The Board of Directors should ensure that an effective AML/CFT programme is in place by establishing appropriate procedures and ensuring their effective implementation. It should cover proper management oversight, systems and controls, segregation of duties, training of staff and other related matters.
38. Customers who are likely to pose a higher than average risk should be categorised as medium or high risk depending on the background, nature and location of activity, country of origin, sources of funds, customer profile, etc. Customers requiring very high level of monitoring, e.g., those involved in cash intensive business, Politically Exposed Persons (PEPs) of foreign origin, may, if considered necessary, be categorised as high risk.

39. 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.
40. In case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.
41. Banks should ensure that their respondent banks have KYC/AML policies and procedures in place and apply enhanced 'due diligence' procedures for transactions carried out through the correspondent accounts. Banks should 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 not affiliated to any regulated financial group). The correspondent bank should not permit its accounts to be used by shell banks.
42. **Wire Transfer** : Banks/FIs 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 rapid and secure method for transferring value from one location to another.
43. (a) The salient features of a wire transfer transaction are as under: (i) 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 could be the same person. (ii) 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. (iii) 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. (iv) 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.
44. Accordingly, banks/FIs must ensure that all wire transfers are accompanied by the following information: 1. Cross-border wire transfers 2. Domestic wire transfers
45. Cross-border wire transfers (i) All cross-border wire transfers must be accompanied by accurate and meaningful originator information. (ii) Information accompanying cross-border wire transfers must contain the name and address of the originator and where an account exists, the number of that account. In the absence of an account, a unique reference number, as prevalent in the country concerned, must be included. (iii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.
46. **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.50,000/- (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 at (i) above should be included in the message.

47. Role of Ordering, Intermediary and Beneficiary banks

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

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

(iii) **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.

48. **Maintenance of records of transactions :** Banks/FIs should introduce a system of maintaining proper record of transactions prescribed under Rule 3 of Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (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)Series of all cash transactions individually valued below Rupees Ten Lakh, or its equivalent in foreign currency which are that have taken place within a month and the monthly aggregate which exceeds rupees ten lakhs or its equivalent in foreign currency. It is clarified that for determining 'integrally connected transactions' 'all accounts of the same customer' should be taken into account.

1. All transactions involving receipts by non-profit organisations of value more than rupees ten lakh or its equivalent in foreign currency [Ref: Government of India Notification dated November 12, 2009- Rule 3,subrule (1) clause (BA) of PML Rules]
2. 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
3. All suspicious transactions, whether or not in cash, made as mentioned in the Rules

49. Banks/FIs are required to maintain all necessary information in respect of transactions prescribed under PML Rule 3 so as 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.
50. 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.
51. 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 five years after the business relationship is ended as required under Rule 10 of the Rules ibid. The identification of records and transaction data should be made available to the competent authorities upon request.
52. 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.
53. Combating Financing of Terrorism : The United Nations periodically circulates the following two lists of individuals and entities, suspected of having terrorist links, and as approved by its Security Council (UNSC).
(a) The "Al-Qaida Sanctions List", includes names of individuals and entities associated with the Al-Qaida.
(b) The "1988 Sanctions List", consisting of individuals (Section A of the consolidated list) and entities.
54. The United Nations Security Council Resolutions (UNSCRs), received from Government of India, are circulated by the Reserve Bank to all banks and FIs. Banks/FIs are required to update the lists and take them into account for implementation of Section 51A of the Unlawful Activities (Prevention) (UAPA) Act, 1967, discussed below.

Banks/FIs should ensure that they do not have any account in the name of individuals/entities appearing in the above lists. Details of accounts resembling any of the individuals/entities in the list should be reported to FIUIND.

55. Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967 :

(a) **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 (Annex II of this circular) detailing the procedure for implementation of Section 51A of the Unlawful Activities (Prevention) Act, 1967 for 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 servicesavailable 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.

57. **Jurisdictions that do not or insufficiently apply the FATF Recommendations**:
(a) Banks/FIs 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/FIs should also consider publicly available information for identifying countries, which do not or insufficiently apply the FATF Recommendations. It is clarified that banks/FIs 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/FIs 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 retained and made available to Reserve Bank/other relevant authorities, on request.

58. In terms of the Rule 3 of the PML (Maintenance of Records) Rules, 2005, banks/FIs are required to furnish information relating to cash transactions, cash transactions integrally connected to each other, and all transactions involving receipts by non-profit organisations (NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered (erstwhile Section 25 of Companies Act, 1956) under Section 8 of the Companies Act, 2013), cash transactions ;where forged or counterfeit currency notes or bank notes have been used as genuine, cross border wire transfer, etc. to the Director, Financial Intelligence Unit-India (FIU-IND).

59. FIU-IND has released a comprehensive reporting format guide to describe the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The Office Memorandum issued on Reporting Formats under Project FINnet dated 31st March, 2011 by FIU containing all relevant details are available on FIU's website. Banks/FIs should carefully go through all the reporting formats prescribed by FIU-IND.

60. FIU-IND have placed on their website editable electronic utilities to file electronic Cash Transactions Report (CTR)/ Suspicious Transactions Report (STR) to enable banks/FIs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore, advised that in cases of those banks/FIs, where all the branches are not fully computerized, the Principal Officer of the bank/FI should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website http://fiuindia.gov.in.

In terms of Rule 8, while furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall constitute a separate violation. Banks/FIs are advised to take note of the timeliness of the reporting requirements.

62. Reports to be furnished to FIU-IND :

1) Cash Transaction Report (CTR)
2) Suspicious Transaction Reports (STR)
3) Non-Profit Organisation
4) Cross-border Wire Transfer

63. The CTR for each month should be submitted to FIU-IND by 15th of the succeeding month. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis and banks/FIs should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.
64. All cash transactions, where forged or counterfeit Indian currency notes have been used as genuine should be reported by the Principal Officer of the bank to FIU-IND in the specified format(Counterfeit Currency Report – CCR), by 15thday of the next month. 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.
65. While filing CTR, details of individual transactions below Rupees Fifty thousand need not be furnished. 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.
66. A summary of cash transaction reports for the bank as a whole should be compiled by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-IND. In case of CTRs compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre, banks may generate centralised CTRs in respect of the branches under core banking solution at one point for onward transmission to FIU-IND, provided the CTR is to be generated in the format prescribed by FIU-IND.
67. A copy of the monthly CTR submitted to FIU-India in respect of the branches should be available at the branches for production to auditors/inspectors, when asked for; and instruction on 'Maintenance of records of transactions'; and 'Preservation of records' should be scrupulously followed by the branches. However, in respect of branches not under CBS, the monthly CTR should continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND.
68. 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/FIs should report all such attempted transactions in STRs, even if not completed by the customers, irrespective of the amount of the transaction.
69. 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.
70. Banks/FIs should not put any restrictions on operations in the accounts where an STR has been filed. Banks/FIs 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.
71. 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.
72. 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 fund is in India.
73. Banks/FIs may nominate a Director on their Boards as "designated Director", as required under provisions of the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (Rules), to ensure compliance with the obligations under the Act and Rules. The name, designation and address of the Designated Director may be communicated to the FIU-IND. UCBs/ State Cooperative Banks / Central Cooperative Banks can also designate a person who holds the position of senior management or equivalent as a 'Designated Director'. However, in no case, the Principal Officer should be nominated as the 'Designated Director'.
74. Principal Officer: Banks/FIs may appoint a senior officer as Principal Officer (PO). The PO should be independent and report directly to the senior management or to the Board of Directors. The PO shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required

under the law/regulations. The name, designation and address of the Principal Officer may be communicated to the FIU-IND.

75. **The Unlawful Activities (Prevention) Act, 1967 (UAPA)** has been amended and notified on 31.12.2008, which, inter-alia, inserted Section 51A to the Act. Section 51A reads as under:-"51A. For the prevention of, and for coping with terrorist activities, the Central Government shall have power to – (a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism; (b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism; (c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.
76. The Unlawful Activities (Prevention) Act define "Order" as under:- "Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time. In order to expeditiously and effectively implement the provisions of Section 51A, the following procedures shall be followed:-
77. Appointment and Communication of details of UAPA nodal officers

As regards appointment and communication of details of UAPA nodal officers -

(i) The UAPA nodal officer for IS-I division would be the Joint Secretary (IS.I), Ministry of Home Affairs. His contact details are 01123092736(Tel), 011-23092569(Fax) and e-mail. (ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA nodal officer and communicate the name and contact details to the IS-I Division in MHA. (iii) The States and UTs should appoint a UAPA nodal officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the IS-I Division in MHA. (iv) The IS-I Division in MHA would maintain the consolidated list of all UAPA nodal officers and forward the list to all other UAPA nodal officers. (v) The RBI, SEBI, IRDA should forward the consolidated list of UAPA nodal officers to the banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies respectively. (vi) The consolidated list of the UAPA nodal officers should be circulated to the nodal officer of IS-I Division of MHA in July every year and on every change. Joint Secretary(IS-I), being the nodal officer of IS-I Division of MHA, shall cause the amended list of UAPA nodal officers to be circulated to the nodal officers of Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, RBI, SEBI, IRDA and FIU-IND.

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

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

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

(iii) The banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU-IND, as the case may be.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt, the banks stock exchanges / depositories, intermediaries regulated by SEBI and insurance

companies would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts

79. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND.
80. In case, the designated individuals/entities are holding financial assets or economic resources of the nature of immovable property and if any match with the designated individuals/entities is found, the UAPA nodal officer of the State/UT would cause communication of the complete particulars of such individual/entity along with complete details of the financial assets or economic resources of the nature of immovable property to the Joint Secretary (IS.I), Ministry of Home Affairs, immediately within 24 hours.

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

82. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the State/UT.

83. **Implementation of requests received from foreign countries under U.N. Security Council Resolution 1373 of 2001.** : U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

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. The UAPA nodal officer of IS-I Division of MHA, shall cause the request to be examined, within 5 working days so as to satisfy itself that on the basis of applicable legal principles, the requested designation is supported by reasonable grounds, or a reasonable basis, to suspect or believe that the proposed designee is a terrorist, one who finances terrorism or a terrorist organization, and upon his satisfaction, request would be electronically forwarded to the nodal officers in Regulators. FIU-IND and to the nodal officers of the States/UTs. The proposed designee, as mentioned above would be treated as designated individuals/entities. The freezing orders shall take place without prior notice to the designated persons involved.

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

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

The banks stock exchanges/depositories, intermediaries regulated by SEBI, insurance companies, Registrar of Immovable Properties and the State/UT nodal officers shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details 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 15 working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States/UTs. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

85. **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, depositories/stock exchanges, intermediaries regulated by SEBI, insurance companies through respective Regulators, and to all the Registrars performing the work of registering immovable properties, through the State/UT nodal officer by IS-I Division of MHA.

86. Regarding prevention of entry into or transit through India : As regards prevention of entry into or transit through India of the designated individuals, the Foreigners Division of MHA, shall forward the designated lists to the immigration authorities and security agencies with a request to prevent the entry into or the transit through India. The order shall take place without prior notice to the designated individuals/entities. The immigration authorities shall ensure strict compliance of the Orders and also communicate the details of entry or transit through India of the designated individuals as prevented by them to the Foreigners' Division of MHA.

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

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

88. **Clients of special category (CSC)**: Such clients include the following-

i. Non resident clients

ii. High net-worth clients,

iii. Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations

a. Companies having close family shareholdings or beneficial ownershipPolitically Exposed Persons (PEP) are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc.

b. Companies offering foreign exchange offerings

vii. Clients in high risk countries where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, countries active in narcotics production, countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, countries against which government sanctions are applied, countries reputed to be any of the following – Havens/ sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent. While dealing with clients in high risk countries where the existence/effectiveness of money laundering control is suspect, intermediaries apart from being guided by the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf- gafi.org), shall also independently access and consider other publicly available information.

viii. Non face to face clients

Clients with dubious reputation as per public information available etc. The above mentioned list is only illustrative and the intermediary shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not

AMLKYC Recollected Questions and Exam Tips::::

Kindly focus on case studies in Macmillan, international organization for AML, FATF latest recommendations,PMLA act latest developments, Reports sent to FIU_IND

1.high medium low risk categories kyc review period 3 questions came directly
2.Gave example of transactions and asked wat type of money laundering is that-funnel accts,deposit structuring,multiple tier account 3ques
3.IBA study group paper published 3 questions from that
4.Placment,layering, integration 1 case study each topic
5.hawala is wat type of ml

6.ml word is coined by the guardian in -watergate scandal
7.FIU IND based questions 6-8
8.5-7case studies one came from text book itself
9.OVD based questions 3
10.given options with type of customer and the documents they submit and asked which customer is eligible for opening sb
11.reporting entity have-designated director
12.designated director is appointed by
13.report submission questions 3
STR within 7 days
CTR within 15th of next month
14.kyc policy is revised by n within
15.key elements of STR

All 2 marks from case studies.

(Placement

Layering

Integration)

Funnel account

Copy of byelaws

Trust company percentage in shars or.profits

Ration card valid or not

Money laundering acts

Str

Ccr

Ftr

Max punishment for money laundering

Wolfsburg principle

Penality for pmla maintainance of records

How many years records to be maintained

Counterfeit notes more than 5

Dormant accounts

Customer not giving info abt the account, what action we have to take

Fatf

Banks under Wolfsburg grp

Small accounts max limits

Thresholds 3 questions

Reports around 4 to 5

Fiu ind, fatf around 5

Wire transfer direct questions like max limit, originator information

Front company

Red flag indicator

Risk category 3 questions around

Some direct questions like

Customer definition in kyc norms

Key elements in kyc policy

Non profit organization

Ckycr

Company trust partnership

Overall if we go though MacMillan book it's good enough to clear the exam..

Case studies are scoring part

MCQs

1. .The amount beyond which cash transactions (Receipts & Payments) are to be monitored by the Commercial Banks as stipulated by the RBI in its guidelines is -

A.Rs.5 lacs & above B. Rs.8 lacs & above **C. Rs.10 lacs & above** D. No such limit

2. Submission of details of PAN (Permanent Account Number) is compulsory for Fixed Deposits, Remittances, such as, DDs / TTs/ Rupee TCs, etc., if the amount exceeds –

A. Rs.10,000/- B. Rs.25,000/- **C. Rs.50,000/-** D. No such limit

3. Branches should not open deposit/advances accounts of banned/ terrorist organisations as circulated by -

A.IRDA B. SEBI C. AMFI **D. FIU**

4..FCRA means - **Foreign Contribution Regulation Act**

5..Maximum punishment by way of imprisonment for the offence committed under Money Laundering Act is -

A. 7 years B. 9 years **C. 10 years** D. 12 years

6. "Smurfing" means -

A. large number of cash deposits into same account

B. one voucher for high value deposit

C. low value denominations of cash

D. None of the above

7..The objective of verifying the employee life-styles by the employer is -

b to know the source of income

c to ascertain whether the employee is having any contacts with illegal organisations

C. to ascertain whether the employee is assisting organisations banned by statutory authorities **D. All of these**

8..Role of the concurrent auditors / Internal auditors with KYC is to -

(g) Review of compliance of KYC guidelines

a Effectiveness of the implementation of the KYC

b Verification of newly opened accounts and their transactions

c All of the above

9 .Strict adherence to KYC norms is achieved through -

(c) following the statutory authority guidelines

a identification of customers with appropriate documents

b strict Implementation of the Banks Systems and procedures while opening the accounts

D. All of the above

10.Name the software available in the market for KYC implementation -

A. Bank Master B. Tally **C. Bank Alert** D. Bank Call

11. Which of the following transactions is/are not consistent with a salaried customer's account?

a Frequent deposits of cash in large sums by third parties

b Deposit of cheques issued by foreign companies

c High value transactions routed through the account with high frequency

D. All of the above

12. Which of the following transactions is/are suspicious from AML angle -

a Large volume of credits happen through DDs/TTs/BC etC.,

b Deposit of several small values of cheques

c Frequent deposits of cash into the account by persons other than the account holder or his authorised representative

d All of the above

13. While accounts are transferred from one branch to another, the receiving branch is expected to comply with KYC Norms. Which one of the following is/are correct in this regard?

a Detailed verification of Customer Profile as received from the earlier branch is to be done with caution

b Detailed verification is not needed but the account is opened immediately and informed to the customer

c Fresh details are to be obtained and a fresh customer profile is to be prepared

d No transaction is to be permitted for the first six months till the customer is fully know to the bank

14.One of the sources that is available to identify the correctness of the information given by the New Customer of the Commercial Bank is –

A.Introduction given by the existing customer of the Bank

B. By studying the account opening form

C. By providing information by the agencies like CRISIL

D. None of the above

15 Which of the following is a source of identification of new customer who is not having any valid documents such as, passport, etC.

a Introduction from the third person having an account with the bank /branch

b Introduction given the Safe deposit locker holder of the bank

c Self–declaration given by the new customer along with other opening forms

d None of the above

16 Is India a member of FATF?

A. **Yes B.** NoC. Has applied for inclusion D. Is likely to be made a member

17. Is adopting Anti Money Laundering practices compulsory for Banks in India?

A. Yes B. No C. Not Sure D. Will be made compulsory soon

18 Letter of thanks is sent to introducer/s because it is -

a. laid down in the banks' manual

b. a routine practice followed by banks for years

C. recommended by the Auditors of banks

D. assisting banks in verification of genuineness or otherwise of the address

19. Which of the following is the cardinal rule for bankers in anti-money laundering efforts -

A. Know Your Customer & Know Your Employee

B Know the Customer of the other Banks

C. Know the income of the Customers of your Bank

D. Know the Assets Position of the customers of the Bank

20 Money Laundering means -

a. Conversion of assets to invest in Laundromats

b. Conversion of money which is illegally obtained to make them legitimate

c. Conversion of cash into gold to make them legitimate

d. Conversion of assets into cash to make them legitimate

21 While opening an account in the name of a company, the following document/s is/are to be obtained -

a. Organisation Chart of the company

b. Roles and responsibilities of the Company

c. Memorandum and Articles of Association of the Company

d. Instructions of the Registrar of the Compan

22 How many recommendations were made by FATF on anti money laundering -

A. 65 recommendations B. NIL **C. 40 recommendations** D. Yet to be finalised

23. For opening accounts in the case of Joint Hindu Undivided Family (JHUF), the following document/s is/are important -

a. Declaration of all family members

b. Declaration of the Karta of the family

c. Declaration of all guardians on behalf of minors

d. Declaration can be exempted as per Hindu Succession Act

24. While opening an account in case of partnership firm, one of the vital document to be produced by the firm is -
A. Partners MOU **B. Partnership Deed**

C. Registration certificate of Partnership D. Signatures of the partners

25. Cash cannot be accepted for issue of DDs/TTs/Rupee TCs from the customers for Rs. ____

A. Rs.50,000/- & above B. Rs.75,000/- & above

C. Rs.1,00,000/- & above D. Rs.1,50,000/- & above

26. The branches of commercial banks should report suspicious transactions to -

A. Bank's respective autho B. RBI C. Ministry of Finance D. None of the above

27. Maximum punishment by way of imprisonment for the offence committed under Money Laundering Act is -

A. 7 years B.9 years **C. 10 years** D. 12 years

28. Maximum retention period of the bank records in case of suspicious transactions is -

A. 5 years B. 7 years **C. 10 years** D. 15 years

29. .Four eyes concept means -

A. opening and verifying of account by one person two times

B. opening and verifying of account by electronic device/s

C. opening and verifying of account by two different persons

D. none of the above

30 Role of the concurrent auditors / Internal auditors with KYC is to -

(i) Review of compliance of KYC guidelines

(ii) Effectiveness of the implementation of the KYC

(iii) Verification of newly opened accounts and their transactions

(iv) All of the above

31 Role of the front line employees of a bank in respect of KYC guidelines is to -

(i) Identify customers as per the existing instructions

(ii) Serve with Smile while opening the customer accounts

(iii) Assist the customer in filling-up the account opening forms

(iv) Provide efficient customer service

32 Which of the following transactions is/are not consistent with a salaried customer's account?

(i) Frequent deposits of cash in large sums by third parties

(ii) Deposit of cheques issued by foreign companies

(iii) High value transactions routed through the account with high frequency

(iv) All of the above

33 .Which of the following transactions is/are suspicious from AML angle –

A. Large volume of credits happen through DDs/TTs/BC etC.,

B. Deposit of several small values of cheques

C. Frequent deposits of cash into the account by persons other than the account holder or his authorized representative

D. All of the above

34. While accounts are transferred from one branch to another, the receiving branch is expected to comply with KYC Norms. Which one of the following is/are correct in this regard?

A. Detailed verification of Customer Profile as received from the earlier branch is to be done with caution

B. Detailed verification is not needed but the account is opened immediately and informed to the customer

C. Fresh details are to be obtained and a fresh customer profile is to be prepared

D. No transaction is to be permitted for the first six months till the customer is fully know to the bank

35. Unusual activities in respect of an customers account is/are -

A. Opening of account at a place other than the place of work

B. Frequent deposits of large sums of money bearing labels of other banks into the account

C. Request for closure of newly opened accounts where high value transactions are routed through

D. All of the above

36. For effective implementation of "Know Your Employee", measures to be adopted by the banks are -

Verification of the life-styles of the employees

Proper Job-rotation in work environment

Not allowing frequent cheque purchase to the employees by the employer

All of the above

37. .Indicator/s about the suspicious transactions of a customer accounts is/are -

A. Depositing high value third party cheques endorsed in favour the account holder B. Sudden increase in cash deposits

C. Receipt or payment of large sums of cash, which have no obvious purpose **D. All of the above**

38. .Which of the following document/s that can be accepted by the Banks as a proof of Customer Identification -

A. Electricity Bill B. Salary Slip

C. Income/Wealth Tax Assessment Order **D. All of the above**

39. .Which of the following is a source of identification of new customer who is not having any valid documents such as, passport, etC.

A. Introduction from the third person having an account with the bank /branch

B. Introduction given the Safe deposit locker holder of the bank

C. Self–declaration given by the new customer along with other opening forms

D. None of the above

40. KYC is --

A. A One-time proje B. To be carried out every 5 years

C. To be carried out every 2 years **D. An ongoing process**

41. Is India a member of FATF?

A. Yes **B. No** C. Has applied for inclusion D. Is likely to be made a member

42. .What is the level of risk of Money Laundering in a Liability product (e.g., deposits)?

A. Generally High **B.Medium** C. Generally Low D. Cannot say

43. .Letter of thanks is sent to introducer/s because it is -

A. laid down in the banks' manual B. a routine practice followed by banks for years

C. recommended by the Auditors of banks

D. assisting banks in verification of genuineness or otherwise of the address

44. .While company Opening an account in the name of a company, the following document/s is/are to be obtained

A. Organisation Chart of the Company

B. Roles and responsibilities of the Company

C. Memorandum and Articles of Association of the Company

D. Instructions of the Registrar of the Company

45. .Due diligence is done at the time of opening an account to enable banks to ensure –

A. identification of the customer at the time of opening an account

B. correctness of the various denominations of notes given by the customer while opening an account

C. authenticity of the signatures of the customer at the time of opening an account

D. speeding up the process of account opening of the new customers

46. For opening accounts in the case of Joint Hindu Undivided Family (JHUF), the following document/s is/are important –
A. Declaration of all family members **B. Declaration of the Karta of the family**

C. Declaration of all guardians on behalf of minors

D. Declaration can be exempted as per Hindu Succession Act

47. . While opening an account in case of partnership firm, one of the vital document to be produced by the firm is -

A. Partners MOU **B. Partnership Deed** C. Registration certificate of Partnership D. Signatures of the partners

48. The amount beyond which cash transactions (Receipts & Payments) are to be monitored by the Commercial Banks as stipulated by the RBI in its guidelines is -

A. Rs.5 lacs & aboveB. Rs.8 lacs & above **C. Rs.10 lacs & above** D. No such limit

49. Submission of details of PAN (Permanent Account Number) is compulsory for Fixed Deposits, Remittances, such as, DDs / TTs/ Rupee TCs, etc., if the amount exceeds -

A. Rs.10,000/- B. Rs.25,000/- **C. Rs.50,000/-** D. No such limit

50. The branches of commercial banks should report suspicious transactions to -

A. Bank's respective authority B. RBI C. Ministry of Finance D. None of the above

51. Banks are made accountable for opening an account in the name of terr
. organisation under ------ of POTA 2002

A. Section 16 B. Section 20 **C. Section 18** D. None of the above

52. Which of the following is/are the terrorist organisation/s notified under POTA, 2002

A. Khalistan Zindabad Force B. Deendar Anjuman C. All Tripura Tiger Forc these D. All of

53. FCRA means -

A. Foreign Currency Regulation Act **B. Foreign Contribution Regulation Act**

C. Foreign Cheques / Commodities Regulation Act D. None of the above

54. Dormant / In-operative account means -

(a) No debits / credits in account for certain period

(b) A dead account not operated for over 10 years

(c) No debit entries, but certain credit entries for certain period D. A fixed asset account

55. The objective of verifying the employee life-styles by the employer is -

(a) to know the source of income

(b) to ascertain whether the employee is having any contacts with illegal organisations

(c) to ascertain whether the employee is assisting organisations banned by statutory authorities

(d) All of these

56. Maximum retention period of the bank records in case of suspicious transactions is -

A. 5 years B. 7 years **C. 10 years** D. 15 years

57. Role of the front line employees of a bank in respect of KYC guidelines is to -

(a) Identify customers as per the existing instructions

(b) Serve with Smile while opening the customer accounts

(c) Assist the customer in filling-up the account opening forms

(d) Provide efficient customer service

58. Name the software available in the market for KYC implementation -

A. Bank Master B. Tally **C. Bank Alert** D. Bank Call

59. Unusual activities in respect of an customers account is/are -

1) Opening of account at a place other than the place of work

2) Frequent deposits of large sums of money bearing labels of other banks into the account

C. Request for closure of newly opened accounts where high value transactions are routed through **D. All of the above**

60. . A new customer may be identified through -

A. Passport Card B. Election ID Card C, PAN Card **D. All of the above**

61. One of the sources that is available to identify the correctness of the information given by the New Customer of the Commercial Bank is -

(i) Introduction given by the existing customer of the Bank

(ii) By studying the account opening form

(iii) By providing information by the agencies like CRISIL D. None of the above

62. Objective of KYC guidelines issued by RBI is -

(i) To control the financial frauds/money laundering

(ii) To discourage opening of new accounts

(iii) To increase competition among the public sector and private sector banks

(iv) To check / control over the new accounts

63. Which of the following document/s that can be accepted by the Banks as a proof of Customer Identification -

(i) Electricity Bill B. Salary Slip C. Income/Wealth Tax Assessment Order**D. All of the above**

64. Which of the following is a source of identification of new customer who is not having any valid documents such as, passport, etC.

(i) Introduction from the third person having an account with the bank /branch

(ii) Introduction given the Safe deposit locker holder of the bank

(iii) Self–declaration given by the new customer along with other opening forms

(iv) None of the above

65. Is adopting Anti Money Laundering practices compulsory for Banks in India?

A. Yes B. No C. Not Sure **D. Will be made compulsory soon**

66. Letter of thanks is sent to introducer/s because it is -

(i) laid down in the banks' manual

(ii) a routine practice followed by banks for years

(iii) recommended by the Auditors of banks

(iv) assisting banks in verification of genuineness or otherwise of the address

67. Which of the following is the cardinal rule for bankers in anti-money laundering efforts -

A. Know Your Customer & Know Your Employee

B. Know the Customer of the other Banks

C. Know the income of the Customers of your Bank

D. Know the Assets Position of the customers of the Bank

68. . While opening an account in the name of a company, the following document/s is/are to be obtained - A. Organisation Chart of the company B. Roles and responsibilities of the Company

C. Memorandum and Articles of Association of the Company

D. Instructions of the Registrar of the Company

69. FATF means - **Financial Action Task force**

70. One of the important steps to be taken while opening NRI accounts is …… by the bank branch

a. Authentication / verification of signature by Indian Embassy

b. Authentication / verification of signature made by the relative of NRI in India

C. Authentication / verification of signature made by friends of the NRI who are abroad staying

d. All of the above

71.In case of societies, the important document to be verified is -

A. Copy of Bye-Laws B. Certificate given by the ROC

C. Certificate given by the Local Authorities

D. No document is to be verified in case of societies, as it is exempted

72. The amount beyond which cash transactions (Receipts & Payments) are to be monitored by the Commercial Banks as stipulated by the RBI in its guidelines is -

A. Rs.5 lacs & aboveB. Rs.8 lacs & above **C. Rs.10 lacs & above** D. No such limit

73. .In computerised branches, suitable filters are required in the software for the purpose of -

A. calculating the correct rate of interest B. printing out the customer profiles

C. monitoring the suspicious transactions D. sharing information/data to the Head Office

74. .Banks are made accountable for opening an account in the name of terrorist organisation under ------ of POTA 2002

A.Section16 B. Section20 **C. Section 18** D. None of the above

75.FCRA means -

A. Foreign Currency Regulation Act **B. Foreign Contribution Regulation Act**

C. Foreign Cheques / Commodities Regulation Act D. None of the above

76. Maximum punishment by way of imprisonment for the offence committed under Money Laundering Act is -

A. 7 years B.9 years **C.10 years** D. 12 years

77. Dormant / In-operative account means -

c. No debits / credits in account for certain period

d. A dead account not operated for over 10 years

e. No debit entries, but certain credit entries for certain period D. A fixed asset account

78. .The objective of verifying the employee life-styles by the employer is -

D. All of these

A. to know the source of income

B. to ascertain whether the employee is having any contacts with illegal organisations

C. to ascertain whether the employee is assisting organisations banned by statutory authorities

79. . Maximum retention period of the bank records in case of suspicious transactions is -

A. 5 years B. 7 years **C. 10 years** D. 15 years

80. Role of the concurrent auditors / Internal auditors with KYC is to -

A. Review of compliance of KYC guidelines

B. Effectiveness of the implementation of the KYC

C. Verification of newly opened accounts and their transactions **D. All of the above**

81. Strict adherence to KYC norms is achieved through -

A. following the statutory authority guidelines

B. identification of customers with appropriate documents

C. strict Implementation of the Banks Systems and procedures while opening the accounts

D. All of the above

ix. For effective implementation of "Know Your Employee", measures to be adopted by the banks are -

A. Verification of the life-styles of the employees

B. Proper Job-rotation in work environment

C. Not allowing frequent cheque purchase to the employees by the employer

D. All of the above

f) Indicator/s about the suspicious transactions of a customer accounts is/are -

a Depositing high value third party cheques endorsed in favour the account holder

b Sudden increase in cash deposits

c Receipt or payment of large sums of cash, which have no obvious purpose

d All of the above

g) Which of the following objective/s is/are important under new KYC Norms?

A. To curb Money Laundering B. To curb the specious activities

C. To monitor/check the transactions of the bank customers

D. All of the above

89.The main objective of KYC is to -

A. Prevent Money Laundering activities B. Improve Customer Service

C. Improve Customer Documentation Standards D. None of these

90. Is adopting Anti Money Laundering practices compulsory for Banks in India?

A. Yes B. No C. Not Sure **D. Will be made compulsory soon**

91. Letter of thanks is sent to introducer/s because it is -

A. laid down in the banks' manual B. a routine practice followed by banks for years C. recommended by the Auditors of banks

D. assisting banks in verification of genuineness or otherwise of the address

92. Money Laundering measures were originally introduced by? A. DICGC B. EXIM Bank C. FDIC **D. SEBI**

93.FATF is located at -

A.Mumbai B.New York **C. Paris** D. Japan

94. One of the important steps to be taken while opening NRI accounts is …… by the bank branch

ii) Authentication / verification of signature by Indian Embassy

iii) Authentication / verification of signature made by the relative of NRI in India

iv) Authentication / verification of signature made by friends of the NRI who are staying abroad

v) All of the above

95. In case of societies, the important document to be verified is -

ii) Copy of Bye-Laws B. Certificate given by the ROC

Certificate given by the Local Authorities

No document is to be verified in case of societies, as it is exempted

96. For opening accounts in the case of Joint Hindu Undivided Family (JHUF), the following document/s is/are important - A. Declaration of all family members **B. Declaration of the Karta of the family**

C. Declaration of all guardians on behalf of minors

D. Declaration can be exempted as per Hindu Succession Act

97. In computerised branches, suitable filters are required in the software for the purpose of -

A. calculating the correct rate of interest B. printing out the customer profiles

C. monitoring the suspicious transactions

D. sharing information/data to the Head Office

98. The objective of verifying the employee life-styles by the employer is - A. to know the source of income

B. to ascertain whether the employee is having any contacts with illegal organisations

C. to ascertain whether the employee is assisting organisations banned by statutory authorities

D. All of these

99. Strict adherence to KYC norms is achieved through -

following the statutory authority guidelines

identification of customers with appropriate documents

strict Implementation of the Banks Systems and procedures while opening the accounts

All of the above

100. Role of the front line employees of a bank in respect of KYC guidelines is to -

Identify customers as per the existing instructions

Serve with Smile while opening the customer accounts

Assist the customer in filling-up the account opening forms

Provide efficient customer service

101. While accounts are transferred from one branch to another, the receiving branch is expected to comply with KYC Norms. Which one of the following is/are correct in this regard?

Detailed verification of Customer Profile as received from the earlier branch is to be done with caution

Detailed verification is not needed but the account is opened immediately and informed to the customer

Fresh details are to be obtained and a fresh customer profile is to be prepared

No transaction is to be permitted for the first six months till the customer is fully know to the bank

102. Unusual activities in respect of an customers account is/are -

Opening of account at a place other than the place of work

Frequent deposits of large sums of money bearing labels of other banks into the account

Request for closure of newly opened accounts where high value transactions are routed through D. All of the above

103. For effective implementation of "Know Your Employee", measures to be adopted by the banks are -

Verification of the life-styles of the employees B. Proper Job-rotation in work environment

C. Not allowing frequent cheque purchase to the employees by the employer D. All of the above

104. Objective of KYC guidelines issued by RBI is -

To control the financial frauds/money laundering

To discourage opening of new accounts

To increase competition among the public sector and private sector banks

To check / control over the new accounts

105. Which of the following is a source of identification of new customer who is not having any valid documents such as, passport, etC.

Introduction from the third person having an account with the bank /branch

Introduction given the Safe deposit locker holder of the bank

Self–declaration given by the new customer along with other opening forms

None of the above

106. Which of the following is the cardinal rule for bankers in anti-money laundering efforts -

Know Your Customer & Know Your Employee B. Know the Customer of the other Banks

C. Know the income of the Customers of your Bank

D. Know the Assets Position of the customers of the Bank

107. Money Laundering means -

Conversion of assets to invest in Laundromats

Conversion of money which is illegally obtained to make them legitimate

Conversion of cash into gold to make them legitimate

Conversion of assets into cash to make them legitimate

108. Due diligence is done at the time of opening an account to enable banks to ensure -

identification of the customer at the time of opening an account

correctness of the various denominations of notes given by the customer while opening an account C. authenticity of the signatures of the customer at the time of opening an account

D. speeding up the process of account opening of the new customers

109. The term "Hawala" is an ----- word

A. Telugu B. English **C. Arabic** D. Islamic

110. Money Laundering measures were originally introduced by?

A. DICGC B. EXIM Bank C. FDIC **D. SEBI**

111. One of the important steps to be taken while opening NRI accounts is …… by the bank branch

A. Authentication / verification of signature by Indian Embassy

B. Authentication / verification of signature made by the relative of NRI in India

C. Authentication / verification of signature made by friends of the NRI who are staying abroad

D. All of the above

112. For opening accounts in the case of Joint Hindu Undivided Family (JHUF), the following document/s is/are important -

A. Declaration of all family members

B. **Declaration of the Karta of the family**

C. Declaration of all guardians on behalf of minors

D. Declaration can be exempted as per Hindu Succession Act

MAQ Test 2:

1. Money Laundering measures were originally introduced by?
1. DICGC
2. EXIM Bank
3. FDIC
4. SEBI*

2. Strict adherence to KYC norms is achieved through
1. following the statutory authority guidelines
2. identification of customers with appropriate documents
3. strict Implementation of the Banks Systems and procedures while opening the accounts
4. All of the above*

3. The term "Hawala" is an —— word
1. Telugu
2. English
3. Arabic*
4. Islamic

4. FATF is located at
1. Mumbai
2. New York
3. Paris*
4. Japan

5. The main objective of KYC is to
1. Prevent Money Laundering activities*
2. Improve Customer Service
3. Improve Customer Documentation Standards
4. None of these

6. Maximum retention period of the bank records in case of suspicious transactions is –
1. 5 years
2. 7 years
3. 10 years*
4. 15 years

7. FCRA means
1. Foreign Currency Regulation Act
2. Foreign Contribution Regulation Act*
3. Foreign Cheques / Commodities Regulation Act
4. None of the above

8. Is adopting Anti Money Laundering practices compulsory for Banks in India?
1. Yes
2. Will be made compulsory soon*
3. Not Sure
4. No

9. Objective of KYC guidelines issued by RBI is –
1. To control the financial frauds/money laundering
2. To discourage opening of new accounts
3. To increase competition among the public sector and private sector banks
4. To check / control over the new accounts*

10. Strict adherence to KYC norms is achieved through –
1. following the statutory authority guidelines
2. identification of customers with appropriate documents
3. strict Implementation of the Banks Systems and procedures while opening the accounts
4. All of the above*

11. While opening an account in case of partnership firm, one of the vital document to be produced by the firm is –
1. Partners MOU
2. Partnership Deed*
3. Registration certificate of Partnership
4. Signatures of the partners

12.Name the software available in the market for KYC implementation –
1. Bank Master
2. Tally
3. Bank Alert*
4. Bank Call

13. Smurfing means –
1. large number of cash deposits into same account*
2. one voucher for high value deposit
3. low value denominations of cash
4. None of the above

14. Which of the following is a source of identification of new customer who is not having any valid documents such as, passport, etc.
1. Introduction from the third person having an account with the bank /branch*
2. Introduction given the Safe deposit locker holder of the bank
3. Self–declaration given by the new customer along with other opening forms
4. None of the above

15. Banks are made accountable for opening an account in the name of terrorist organisation under —— of POTA 2002
1. Section 16
2. Section 20
3. Section 18*
4. None of the above

16.In case of societies, the important document to be verified is _____.
1. Certificate given by the Local Authorities
2. Certificate given by ROC
3. Copy of bye laws*
4. No document is to be verified in case of societies

17.Dormant/ in operative account means _____.
1. No debits/credits in account for a certain period*
2. Dead Account without any operation for long
3. No debit entries
4. Fixed asset account of the bank

18. PAN (Permanent Account Number) is compulsory for Fixed Deposits, Remittances like DDs/TTs/RTCs, etc _____.
1. if the amount exceeds Rs 50,000*
2. if the amount exceeds Rs.25
3. if the amount exceeds Rs.10
4. no such limit is fixed by income tax authorities

19. _____ are fake companies that appear on paper, but may not physically exist.
1. Front Companies
2. Offshore Banking
3. Hawala Systems
4. Shell Companies*

20. Which of the following are methods of layering?
1. Deposits and withdrawals are made continuously in their accounts to vary the amount of balance in the accounts
2. Transferring money through various financial institutions among different names in different financial institutions
3. Changeover to different currencies
4.All of the above*

21.Money Laundering refers to _____.
1. Conversion of assets into cash to avoid income tax
2. Tansfer of assets/cash from one account to another
3. Conversion of illegal money through banking channels*
4. Conversion of cash into gold for hoarding

22. While opening an account of a Public Limited company, which of the following is a must?
1. Introduction by ROC
2. Certificate of incorporation/Certificate of commencement of business*
3. Introduction by a customer known to the banker
4. None of the above

23. _____ is the process of keeping the amount lower than that fixed for reporting and building similar transactions till the amount planned to be laundered is reached fully.
1. Slushing
2. Lading
3. Smurfing*
4. Entrailing

24.What is not audited by Internal Audit and Control teams of the banks
1. adequacy of policies
2. adequacy of procedures
3. system support to detect suspicious and potential money laundering transaction
4. None of the above*

25.Which section of PMLA, 2012 provides for Powers of Director to impose fine
1. sec 11
2. sec 12
3. sec 13*
4. sec 14

26.What are not the responsibility of the senior management
1. Appointment of PO
2. Managing the risk of money laundering
3. Internal Reporting Procedures
4. None of the above*

27. Which PMLA rule along with rule 8 requires the reporting of all cash transactions where forged or counterfeit Indian currency notes have been used as genuine
1. 1
2. 2
3. 3*
4. 4

28.Who enlists the format of CTR
1. SEBI
2. RBI*
3. Ministry of Finance
4. Ministry of Company Affairs

29. Which of these activities might require a suspicious activity report?
1. A customer cancels a transaction and requests to do a second transaction for less amount in order to avoid providing ID
2. A customer requests an unusually high value transaction and cannot explain the reason for the transaction or the source of cash
3. Both A and B above*
4. None of the above

30.Which part of the STR is the 'Soul' of the STR
1. POS
2. GOS*
3. TOS
4. LOS

KYC aml:: Very important

1. Cash receipt or cash payment of more than Rs 10 lakh are reported to FIU on CTR statement which should be sent to FIU within _____ from the close of the month: 15 days.
2. Suspicious Transaction report is sent to FIU within: 7 days from confirmation of suspicion.
3. 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 whether conducted as a single transaction or several transactions that appear to be connected, the customer's identity and address should be verified: fifty thousand
4. As per KYC norms, banks are required to periodical update data. In respect of High risk customers, full KYC exercise will be required to be done at least every: two years
5. As per KYC norms, for how much period banks are required to preserve records in respect of photograph and proof of address or identity?: 5 years from date of close of account
6. As per KYC norms, in the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within: two weeks of such a change
7. As per KYC norms, risk classification of customers should be reviewed in every: 6 Months
8. Banks are required to FIU, cash transactions which are integrally connected to each other and total amount of receipt or total amount of payment in a month is more than: Rs 10 lac
9. Cash Transaction Report (CTR) in respect of cash receipt or cash payment of more than Rs 10 lac is to be sent to Director – FIU. What is the periodicity of the report – Fortnightly, Monthly, Quarterly, half yearly: Monthly, within 15 days of the close of the month.
10.FIR to be filed if number of Counterfeit notes in a single deposit is: 5 or above
11. If a customer does not comply with KYC requirements despite repeated reminders by banks, banks should impose 'partial freezing' by allowing all credits and disallowing all debits with the freedom to close the accounts after ____ months notice followed by a reminder for further period of ____months. If the accounts are still KYC non-compliant after _____months of imposing initial 'partial freezing' banks may disallow all debits and credits from/to the accounts, rendering them inoperative: 3, 3, 6 months.
12.In a cash deposit made by a customer, one piece of counterfeit note is detected. What should the bank do - (i) It should be impounded and acknowledgement to be issued(ii) Should be destroyed (iii) Should be returned back: It should be impounded and acknowledgement to be issued to depositor signed by cashier.
13. In case of counterfeit notes received in a deposit by a person with bank, FIR is not lodged and only a monthly consolidated report is sent if counterfeit notes in one remittance is up to: 4
14.In case of Non-KYC compliant customer, after how much time notice, account should be freezed?: 3 months notice
15.In respect of Low Risk customers, KYC norms relating to obtaining photograph and proof of address and ID should be applied once in: 10 Years
16.In respect of Medium Risk customers, KYC norms relating to obtaining photograph and proof of address and ID should be applied once in: 8 Years
17.Process of making illegally-gained proceeds (i.e. "dirty money") appear legal (i.e. "clean") is called: Money Laundering
18.RBI has allowed banks to accept at least _____ of the documents prescribed by RBI as activity proof by a proprietary concern, for opening a bank account in respect of a sole proprietary firm: One
19. What is the Risk category of Trust account High/Low/medium risk?: High Risk

20.When in case of deposit of cash over counter, two counterfeit notes are detected by bank, what should the bank do – (a) To be returned to customer, (b) impounded immediately, (c) call the police, (d) destroy it: impound immediately and issue acknowledgement totender signed by the cashier
21.While opening bank account, as per KYC norms, what another document is taken by bank in addition to proof of ID?: proof of address (Both can be same also)
22.Relaxation in KYC norms is permitted if the depositor undertakes that the balance outstanding in his account will not be more than and credits in a financial year will not exceed . Rs 50,000; Rs 100,000
23.Why KYC guidelines have been issued by RBI under section 35 A of the Banking Regulation Act: To prevent Money Laundering -
24. The terms used for hiding money to avoid tax is : Money laundering
25. Money laundering: conversion of illegal money into legal through banking channels.
26. For the purpose of KYC rules any addition & modification on which recommendation: Financial Action Task Force
27.Risk type for customer having political exposed person: High Risk
28.As per KYC Guidelines, Records of transactions to be maintained for at least ten years from the dateof transaction, instead of _____from the date of cessation of transactions, and records pertaining to identification of the customer and his address to be preserved for at least ten years after the business relationship is ended: ten years
29.A customer who does not complete all KYC norms, what type of account is opened for him? No Frill account in which cannot be more than Rs.50000 and credits in the Financial Year cannot be more than Rs.100000.
30. There were three cash withdrawals of Rs 5.80 lac ,Rs 4.90 lac & 0.25 lacs from an account in a month. Which of these transactions is/are will be reported to Financial Intelligence Unit as part of CTR? Cash withdrawals of Rs 5.8 lac and Rs 4.9 lac.
31. Under Prevention of Money Laundering Act, banks are required to preserve records relating to opening the account for how much period?: 10 years from date of closure of account.
32.Which of the following is not the key element of KYC policy a) Customer Acceptance Policy; b) Customer Identification Procedures; c) Monitoring of Transactions; d) Risk Management e) Customer Awareness Policy: Ans is E i.e. Customer Awareness Policy.
33. On whose recommendations, KYC norms came into force? (a) Goiporia Committee (b) Ghosh Committee (c) FATF: Ans is FATF
34. Under KYC Norms, Documents relating to opening the account like proof of address and identity and photograph should be taken again at what interval? (a) once in 10 years for low risk customer (b) once in 8 years for medium risk customers (c) once in 1 year for high risk customers (d) Both (a) and (b): Ans is (d)
35.Record of cash receipt and payment under KYC to be maintained if cash receipt or payment in a single day from one account is more than Rs 10 lakh.
36. For Low Risk customers, periodical up-dation of KYC data: Once in 10 years.

Case Study

As we know banks and financial institutions are constantly committed to stop money laundering by fulfilling the KYC norms of the customers. It helps in banks to know the customer as well as help them to satisfy their needs. By KYC norms bank can cross sale and up sale their product to the targeted group segment.

Q.1 What are the minimum time to revise KYC in A/c= 2 Years

Q.2 What is the time period for revise KYC to Low risk, Medium risk and High risk customer consecutively- Ans : 10 : 8 : 2 Years

Q.3 What can be used as an official valid document for KYC purposes?
i) PAN CARD ii) JOB CARD issued by NREGA iii) RATION CARD

Q.4 If a customer opens a small saving bank account without fulfilling KYC Norms. His annually dr. cr kitne honge

Note::Below cases for analysis for knowledge only. Its not a question and answers

KYC AML CASE STUDIES analysis:::

Intermediaries – case study 1

A person (later arrested for drug trafficking) made a financial investment (life insurance) of USD 250,000 by means of an insurance broker. He acted as follows. He contacted an insurance broker and delivered a total amount of USD 250,000 in three cash instalments. The insurance broker did not report the delivery of that amount and deposited the three instalments in the bank. These actions raised no suspicion at the bank, since the insurance broker was known to them as being connected to the insurance branch. The insurance broker delivered, afterwards, to the insurance company responsible for making the financial investment, three cheques from a bank account under his name, totalling USD 250,000, thus avoiding raising suspicions with the insurance company.

Intermediaries – case study 2

Clients in several countries used the services of an intermediary to purchase insurance policies. Identification was taken from the client by way of an ID card, but these details were unable to be clarified by the providing institution locally, which was reliant on the intermediary doing due diligence checks. The policy was put in place and the relevant payments were made by the intermediary to the local institution. Then, after a couple of months had elapsed, the institution would receive notification from the client stating that there was now a change in circumstances, and they would have to close the policy suffering the losses but coming away with a clean cheque from the institution. On other occasions the policy would be left to run for a couple of years before being closed with the request that the payment be made to a third party. This was often paid with the receiving institution, if local, not querying the payment as it had come from another reputable local institution.

Collusion – case study 3

An insurer in collusion with an insured person attempted to launder money through insurance transactions. The manager of an insurance company sold health and personal injury insurance policies insuring against the liability from accidents to dummy persons, normally in the names of friends and relatives. These persons paid a low premium rate. Subsequently claims were received, supported by false documentation and medical certificates to substantiate the losses and the insurer paid the claims promptly. The claims for damages were considerable. The manager then sought to legalise this scheme and recover the damages paid out. Under subrogation rights, the insurance company took legal action against all businesses where the alleged accidents had occurred. The businesses involved (restaurants, clubs etc.) responded that they had not been aware of the alleged accidents and that no such accidents had occurred at the times stated.

Collusion – case study 4

A drug trafficker purchased a life insurance policy with a value of USD 80,000. The policy was purchased through an agent of a large life insurance company using a cashier's cheque. The investigation showed that the client had made it known that the funds used to finance the policy were the proceeds of drug trafficking. In light of this fact, the agent charged significantly higher commission. Three months following this transaction, the investigation showed that the drug dealer cashed in his policy.

Reinsurance – case study 5

An insurer in Country A sought reinsurance with a reputable reinsurance company in Country B for its directors and officers cover of an investment firm in Country A. The insurer was prepared to pay four times the market rate for this reinsurance cover. This raised the suspicion of the reinsurer which contacted law enforcement agencies.

Investigation made clear that the investment firm was bogus and controlled by criminals with a drug background. The insurer had ownership links with the investment firm. The impression is that – although drug money would be laundered by a payment received from the reinsurer – the main purpose was to create the appearance of legitimacy by using the name of a reputable reinsurer. By offering to pay above market rate the insurer probably intended to assure continuation of the reinsurance arrangement.

Reinsurance – case study 6

A group of persons with interests in home construction effected a payment in favour of construction company A under contracts connected with their participation in investment construction (at cost price). Insurance company P accepted possible financial risks to these contracts under a contract of financial risks insurance and received an insurance premium. At the same time the insurance company P concluded with the construction company A a secret agreement providing that the difference between the market cost of housing and the cost price was transferred in favour of the insurance company as a premium under the contract of financial risks insurance. When the funds were received by the insurance company P they were transferred as insurance premium under the general reinsurance contract in favour of insurance company X. By way of fictitious service contracts and commission payments made under an agency contract, insurance company X channelled the funds to several off-shore shell firms. Beneficiaries of the actual profit, being withdrawn abroad, were owners and directors of the construction company A.

KYC AML CASE STUDY ANALYSIS:

A drug trafficker purchased a life insurance policy with a value of USD 80,000. The policy was purchased through an agent of a large life insurance company using a cashier's cheque. The investigation showed that the client had made it known that the funds used to finance the policy were the proceeds of drug trafficking. In light of this fact, the agent charged significantly higher commission. Three months following this transaction, the investigation showed that the drug dealer cashed in his policy.

KYC AML CASE STUDY ANALYSIS:

Two life insurance policies were bought for a large amount in the names of Mr X and Mr Y. The payments were made by cheque, originating from the account of a investment company. Both polices were used as security for a mortgage loan with a company that specialised in leasing. As the beneficiaries were not the policyholders and in light of the unusual financing being provided by a leasing company, the insurer contacted the investment company in order to understand the origin of the money that had been deposited in the account. It appeared that the money was deposited with the company in cash by random clients. Following the disclosure of suspicion by the insurance company it became evident that Mr X and Mr Y were known by the customs authorities for the illegal importation and exportation of cars

KYC AML CASE STUDY ANALYSIS:

A 34 year old car dealer received a loan through a broker of a life insurance company to purchase a house. He invested around 25% of the loan in a single-premium life insurance policy. He later surrendered the policy early to pay back the loan (capital and interest), making up the shortfall through other funds. The use of a substantial proportion of the loan to purchase a policy combined with the unexpectedly early repayment of the loan led to the FIU being contacted. The FIU's investigation revealed that the policyholder was known for stealing and receiving stolen cars. Moreover, he had used false documents to prove the sources of his income and wealth

KYC AML CASE STUDY ANALYSIS:

Two life insurance policies were bought for a large amount in the names of Mr X and Mr Y. The payments were made by cheque, originating from the account of a investment company. Both polices were used as security for a mortgage loan with a company that specialised in leasing. As the beneficiaries were not the policyholders and in light of the unusual financing being provided by a leasing company, the insurer contacted the investment company

in order to understand the origin of the money that had been deposited in the account. It appeared that the money was deposited with the company in cash by random clients. Following the disclosure of suspicion by the insurance company it became evident that Mr X and Mr Y were known by the customs authorities for the illegal importation and exportation of cars

KYC AML CASE STUDY ANALYSIS:

Mrs T (teacher) from country A, entered into a life insurance policy with a small initial premium being paid. The transaction was arranged by Mr B who was the agent of insurance company C and a cousin of Mrs T. Two days later, company C made a payment of an additional premium, in excess of 540,000, on behalf of Mrs T. After one month, Mrs T cancelled her policy and transferred the refund of contributions to three different accounts:
a) Mr MD (Managing Director of Company C) – 240,000;
b) Mrs N (niece of Mr MD) – 150,000; and
c) Mr U – 150,000.
All of them subsequently transferred the money onwards to other accounts in different banks. Following an investigation it appeared that the money being laundered was linked to fuel smuggling. The accounts were blocked by the Financial Intelligence Unit (FIU) and the case was forwarded to the public prosecutor.

Prevention of Money Laundering (Maintenance of Records) Rules, 2005 Amendments vide Notification dated 1st June 2017 PMLA

Salient Highlights

The Prevention of Money Laundering (Maintenance of Records) Rules 2005 have been amended vide Gazette Notification dated 1st June 2017. Consequential, modifications in RBI KYC Directions are yet to be issued. This memo captures the highlights of the amendments made. Only those aspects that have been changed are enumerated below. Other provisions continue to be as already stated in these Rules.

Changes Made:

(1) 'Officially Valid Document' (OVD) definition amended – the Permanent Account Number (PAN) Card; and the letter issued by the Unique Identification Authority of India have been removed from this definition.
(2) Now OVD definition includes - the passport, the driving licence, the Voter's Identity Card issued by Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the National Population Register containing details of name, address or any other document as notified by the Central Government in consultation with the Regulator;
(3) KYC Document Requirement for an Individual changed –
(a) An individual eligible for Aadhaar number is required to submit (i) the Aadhaar number (AN); (ii) the Permanent Account Number (PAN) or Form No. 60.
(b) An individual (eligible for AN), who does not have AN, is required to submit (i) proof of application of enrolment for Aadhaar (in lieu of AN) and (ii) PAN (and not Form 60). (c) An individual (eligible for AN), who does not have both AN and PAN, is required to submit (i) proof of application of enrolment for Aadhaar (in lieu of AN), (ii) one certified copy of an OVD, and (ii) Form 60.
(d) An individual not eligible for AN is required to submit PAN.
(e) An individual, who is not eligible for AN and does not have PAN, is required to submit (i) one certified copy of an OVD, (ii) Form 60, and (iii) one recent photograph .
(f) An individual is also required to submit such other documents (including in respect of the nature of business and financial status of the client) as may be required by the reporting entity (bank, etc.) (also in earlier rules).
(h) In case of 'small accounts' on suspicion of money laundering/ terrorism financing/ other high risk scenarios to establish identity of the individual customer through (i) an OVD, and (ii) AN, and where AN has not been obtained proof of application for AN.

(i) In case of 'small accounts' on completion of initial 12 month period or additional 12 month period (as the case may be) to obtain an OVD. (as per earlier rules)

(4) KYC Requirement for juridicial entities – These have been modified in repsect of KYC documents pertaining to individuals connected with these entities. Instead of an OVD (as per earlier rules) the requirements for the concerned persons are as indicated below.

<table>
<tr><th>S. No.</th><th>Type of Entity</th><th>To obtain in respect of</th><th>KYC Requirement</th></tr>
<tr><td>1</td><td>Company</td><td>managers, officers or employees holding an attorney to transact on the company's behalf</td><td rowspan="4">(a) (i) AN, and (ii) PAN/ Form 60.
(b) If does not have AN, (i) proof of application of enrolment for Aadhaar (in lieu of AN) and (ii) PAN (and not Form 60)
(c) If does not have both AN and PAN, (i) proof of application of enrolment for Aadhaar (in lieu of AN), (ii) one certified copy of an OVD, and (ii) Form 60.
(d) If not eligible for AN and does not have PAN, is required to submit (i) one certified copy of an OVD, and (ii) Form 60.</td></tr>
<tr><td>2</td><td>Partnership Firm</td><td rowspan="3">person holding an attorney to transact on its behalf</td></tr>
<tr><td>3</td><td>Trust</td></tr>
<tr><td>4</td><td>Unincorporated association or Body of individuals</td></tr>
</table>

(5) On receiving AN to carry out authentication using either e-KYC or Yes/No authentication facility provided by Unique Identification Authority of India (UIDAI).

(6) NRIs and residents in the States of Jammu and Kashmir, Assam or Maghalaya who do not submit PAN to submit (i) one certified copy of an OVD, and (ii) photograph and (iii) such other document including in respect of the nature of business and financial status as may be required by the reporting entity.

(7) If a person eligible for AN and PAN does not submit these at the time of commencement of an account based relationship, should submit the same within a period of six months from the date of the commencement of the account based relationship. If AN and PAN are not submitted within 6 months, the said account shall cease to be operational till submitted.

(8) For existing clients, eligible for AN and PAN should submit these by 31st December, 2017. If AN and PAN are not submitted by 31st December, 2017, the said account shall cease to be operational till submitted.

(9) In case the identity information relating to AN and PAN does not have current address of the client, the client shall submit an OVD to the reporting entity.

Additional and important material::

Index

2.11	Operation of bank account and Money Mules
2.12	Bank no longer knows the true identity
2.13	Monitoring of Transactions
2.14	Closure of accounts
2.15	Risk Management
2.16	Introduction of new technology – credit/debit/smart/gift card
2.17	Combating Financing of Terrorism
2.18	Freezing of Assets under Section 51A of Unlawful Activities (Prevention) Act, 1967
2.19	Jurisdictions that do not or insufficiently apply the FATF Recommendations
2.20	Correspondent Banking
2.21	Applicability to branches and subsidiaries outside India
2.22	Wire Transfers
2.23	Designated Director and Principal Officer
2.24	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)
2.25	Cash and Suspicious Transaction Report
2.26	Customer Education/Training of Employees/Hiring of Employees
	Annexures
	Annex - I - Indicative List of documents required for opening of accounts
	Annex-II – UAPA Order dated August 27, 2009
	Annex-III – Government of India, Notification dated December 16, 2010
	Annex – IV – List of circulars consolidated in the Master Circular

20. Introduction

1.1. Know Your Customer (KYC) Norms/Anti-Money Laundering (AML) Measures/Combating of Financing of Terrorism (CFT)/Obligations of banks under PMLA, 2002

The objective of KYC/AML/CFT guidelines is to prevent banks from being used, intentionally or unintentionally, by criminal elements for money laundering or terrorist financing activities. KYC procedures also enable banks to know/understand their customers and their financial dealings better which in turn help them manage their risks prudently.

1.2. Definition of Customer

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

d a person or entity that maintains an account and/or has a business relationship with the bank;

e one on whose behalf the account is maintained (i.e. the beneficial owner). [Ref: Government of India Notification dated February 12, 2010 - Rule 9, sub-rule (1A) of PMLA Rules - 'Beneficial Owner' means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted, and includes a person who exercise ultimate effective control over a juridical person]

f beneficiaries of transactions conducted by professional intermediaries, such as Stock Brokers, Chartered Accountants, Solicitors etc. as permitted under the law, and

g any person or entity connected with a financial transaction which can pose significant reputational or other risks to the bank, say, a wire transfer or issue of a high value demand draft as a single transaction.

2 Guidelines

1.General

(d) Banks should keep in mind that the information collected from the customer for the purpose of opening of account is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes. Banks should, therefore, ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer should be sought separately with his/her consent and after opening the account

14. Banks should ensure that any remittance of funds by way of demand draft, mail/telegraphic transfer or any other mode and issue of travellers' cheques for value of Rupees fifty thousand and above is effected by debit to the customer's account or against cheques and not against cash payment

15. With effect from April 1, 2012, banks should not make payment of cheques/drafts/pay orders/banker's cheques bearing that date or any subsequent date, if they are presented beyond the period of three months from the date of such instrument.

16. Banks should ensure that the provisions of Foreign Contribution (Regulation) Act, 2010, wherever applicable, are strictly adhered to.

2.2. KYC Policy

Banks should frame their KYC policies incorporating the following four key elements:

17 Customer Acceptance Policy;

18 Customer Identification Procedures;

19 Monitoring of Transactions; and

iv)Risk Management.

2.3. Customer Acceptance Policy (CAP)

19 Every bank should develop a clear Customer Acceptance Policy laying down explicit criteria for acceptance of customers. The Customer Acceptance Policy must ensure that explicit guidelines are in place on the following aspects of customer relationship in the bank.

a. No account is opened in anonymous or fictitious/benami name.

[Ref: Government of India Notification dated June 16, 2010 Rule 9, sub-rule (1C) - Banks should not allow the opening of or keep any anonymous account or accounts in fictitious name or account on behalf of other persons whose identity has not been disclosed or cannot be verified].

23 Parameters of risk perception are clearly defined in terms of the nature of business activity, location of customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorisation of customers into low, medium and high risk (banks may choose any suitable nomenclature viz. level I, level II and level III). Customers requiring very high level of monitoring, e.g. Politically Exposed Persons (PEPs) may, if considered necessary, be categorised even higher;

iii) Documentation requirements and other information to be collected in respect of different categories of customers depending on perceived risk and keeping in mind the requirements of PML Act, 2002 and instructions/guidelines issued by Reserve Bank from time to time;

iv) 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. Bank may also consider closing an existing account under similar circumstances. It is, however, necessary to have suitable built in safeguards to avoid harassment of the customer. For example, decision by a bank to close an account should be taken at a reasonably high level after giving due notice to the customer explaining the reasons for such a decision.

25. 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 and

(i) 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.

36. Banks 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. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

37. For the purpose of risk categorisation, 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, the policy may require that only the basic requirements of verifying the identity and location of the customer are to be met. Customers that 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. Banks 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. In view of the risks involved in cash intensive businesses, accounts of bullion dealers (including sub-dealers) & jewelers should also be categorized by banks as 'high risk' requiring enhanced due diligence. Other examples of customers requiring higher due diligence include (a) nonresident customers;

38. 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 and (h) those with dubious reputation as per public information available etc. However, NPOs/NGOs promoted by United Nations or its agencies may be classified as low risk customers.

48. In addition to what has been indicated above, banks/FIs 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. Banks/FIs should have policies, controls and procedures, duly approved by their boards, in place to effectively manage and mitigate their risk adopting a risk-based approach. As a corollary, banks would be required to adopt enhanced measures for products, services and customers with a medium or high risk rating. In this regard, banks may use for guidance in their own risk assessment, a Report on Parameters for Risk-Based Transaction Monitoring (RBTM) dated March 30, 2011 which was issued by Indian Banks' Association as a supplement to their guidance note on Know Your Customer (KYC) norms / Anti-Money Laundering (AML) standards issued in July 2009. The IBA guidance also provides an indicative list of high risk customers, products, services and geographies.

49. It is important to bear in mind that the adoption of customer acceptance policy and its implementation should not become too restrictive and must not result in denial of banking services to general public, especially to those, who are financially or socially disadvantaged.

2.4. Customer Identification Procedure (CIP)

49. The policy approved by the Board of banks should clearly spell out the Customer Identification Procedure to be carried out at different stages, i.e., while establishing a banking relationship; carrying out a financial transaction or 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. Banks 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. Such risk-based approach is considered necessary to avoid disproportionate cost to banks and a burdensome regime for the customers. Besides risk perception, the nature of information/documents required would also depend on the type of customer (individual, corporate etc.). For customers that are natural persons, the banks should obtain sufficient identification data to verify the identity of the customer, his address/location, and also his recent photograph. For customers that are legal persons or entities, the bank should (i) verify the legal status of the legal person/entity through proper and relevant documents;

(i) 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; (iii) understand the ownership and control structure of the customer and determine who are the natural persons who ultimately control the legal person.

54. Banks may seek ‘mandatory’ information required for KYC purpose which the customer is obliged to give while opening an account or during periodic updation. Other ‘optional’ customer details/additional information, if required may be obtained separately after the account is opened only with the explicit consent of the customer. The customer has a right to know what is the information required for KYC that she/he is obliged to give, and what is the additional information sought by the bank that is optional. Further, it is reiterated that banks should keep in mind that the information (both ‘mandatory’ – before opening the account as well as ‘optional’- after opening the account with the explicit consent of the customer) collected from the customer is to be treated as confidential and details thereof are not to be divulged for cross selling or any other like purposes.

57. Customer identification requirements in respect of a few typical cases, especially, legal persons requiring an extra element of caution are given in paragraph 2.5 below for guidance of banks. Banks may, however, frame their own internal guidelines based on their experience of dealing with such persons/entities,

normal bankers' prudence and the legal requirements as per established practices. If the bank decides to accept such accounts in terms of the Customer Acceptance Policy, the bank should take reasonable measures to identify the beneficial owner(s) and verify his/her/their identity in a manner so that it is satisfied that it knows who the beneficial owner(s) is/are [Ref: Government of India Notification dated June 16, 2010 - Rule 9 sub-rule (1A) of PML Rules].

d) In this connection, a reference may be made to the circular DBOD.AML.BC. No. 71/14.01.001/2012-13 dated January 18, 2013 wherein the procedure for determination of Beneficial Ownership, as advised by Government of India has been specified.

59. The increasing complexity and volume of financial transactions necessitate that customers do not have multiple identities within a bank, across the banking system and across the financial system. This can be achieved by introducing a unique identification code for each customer. The Unique Customer Identification Code (UCIC) will help banks to identify customers, track the facilities availed, monitor financial transactions in a holistic manner and enable banks to have a better approach to risk profiling of customers. It would also smoothen banking operations for the customers. While some banks already use UCIC for their customers by providing them a relationship number, etc., other banks have not adopted this practice. Banks were therefore, advised to initiate steps for allotting UCIC to all their customers while entering into any new relationships for individual customers to begin with. Existing individual customers were required to be allotted UCIC by end-May 2013. However, in view of difficulties expressed by some banks in implementing UCIC for their customers, for various reasons, and keeping in view the constraints, the time for completing the process of allotting UCIC to existing customers was extended up to March 31, 2014. In this regard a further extension upto **December 31, 2014** has been allowed. Banks have been advised to expedite the procedure and complete the work of allotting UCIC to all the existing individual customers, within the stipulated timeframe. They may chalk out a plan for completing the work and furnish the monthly progress report to their Board. Considering the fact that a period of two years has been allotted for completion of the task, no further extension in this regard would be considered. Further, it is reiterated that UCIC should be allotted to all customers while entering into new relationships.

60. When there are suspicions of money laundering or financing of the activities relating to terrorism or where there are doubts about the adequacy or veracity of previously obtained customer identification data, banks should review the due diligence measures including verifying again the identity of the client and obtaining information on the purpose and intended nature of the business relationship. [Ref: Government of India Notification dated June 16, 2010- Rule 9 sub-rule (1D) of PML Rules].

61. It has been observed that some close relatives, e.g. wife, son, daughter and parents, etc. who live with their husband, father/mother and son, as the case may be, are finding it difficult to open account in some banks

as the utility bills required for address verification are not in their name. It is clarified, that in such cases, banks can obtain an identity document and a utility bill of the relative with whom the prospective customer is living along with a declaration from the relative that the said person (prospective customer) wanting to open an account is a relative and is staying with him/her. Banks can use any supplementary evidence such as a letter received through post for further verification of the address. While issuing operational instructions to the branches on the subject, banks should keep in mind the spirit of instructions issued by the Reserve Bank and avoid undue hardships to individuals who are, otherwise, classified as low risk customers.

66. Norms for furnishing proof of address have been relaxed to allow submitting 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 may 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 may take a declaration of the local address on which all correspondence will be made by the bank with the customer. No proof is required to be submitted for such address for correspondence/local address. This address may be verified by the bank through 'positive confirmation' such as acknowledgment of receipt of (i) letter, cheque books, ATM cards; (ii) telephonic conversation;

(i) visits; etc. In the event of change in this address due to relocation or any other reason, customers may intimate the new address for correspondence to the bank within two weeks of such a change.

70. Some banks insist on opening of fresh accounts by customers when customers approach them for transferring their account from one branch of the bank to another branch of the same bank. Banks are advised that 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 should be allowed to transfer his account from one branch to another branch without restrictions.Banks 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.

71. Banks should carry out periodical updation of KYC information of every customer, which may include the following:

a. Full KYC exercise may 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 may include all measures for confirming identity and address and other particulars of the customer that the bank may consider reasonable and necessary based on the risk profile of the customer.

b. Positive confirmation (obtaining KYC related updates through e-mail/ letter/ telephonic conversation/ forms/ interviews/ visits, etc.), may be completed at least every two years for medium risk and at least every three years for low risk individuals and entities.

c. Fresh photographs to be obtained from minor customer on becoming major.

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

72. An indicative list of the nature and type of documents/information that may be may be relied upon for customer identification is given in Annex-I to this Master Circular.

73. 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 may be accepted as a valid proof of both identity and address.

74. A rent agreement indicating the address of the customer duly registered with State Government or similar registration authority may also be accepted as a proof of address.

n) It has been brought to our notice that the said indicative list furnished in Annex - I, is being treated by some banks as an exhaustive list as a result of which a section of public is being denied access to banking services. Banks are, therefore, advised to take a review of their extant internal instructions in this regard.

2.5. Customer Identification Requirements – Indicative Guidelines

77. **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 a bank 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 bank should verify the identity and address of the customer and also consider filing a suspicious transaction report (STR) to FIU-IND.

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

b) Salaried Employees

In case of salaried employees, it is clarified that with a view to containing the risk of fraud, banks should rely on certificate/letter of identity and/or address issued only from corporate and other entities of repute and should be aware of the competent authority designated by the concerned employer to issue such certificate/letter. Further, **i<u>n addition</u>** to the certificate/letter issued by the employer, banks should insist on at least one of the officially valid documents as provided in the Prevention of Money Laundering Rules (viz. passport, driving licence, PAN Card, Voter's Identity card, etc.) or utility bills for KYC purposes for opening bank accounts of salaried employees of corporate and other entities.

c) Trust/Nominee or Fiduciary Accounts

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

d) Accounts of companies and firms

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

ii Client accounts opened by professional intermediaries

a. When the bank has knowledge or reason to believe that the client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Banks may

hold 'pooled' accounts managed by professional intermediaries on behalf of entities like mutual funds, pension funds or other types of funds. Banks also maintain 'pooled' accounts managed by lawyers/chartered accountants or stockbrokers for funds held 'on deposit' or 'in escrow' for a range of clients. Where funds held by the intermediaries are not co-mingled at the bank and there are 'sub-accounts', each of them attributable to a beneficial owner, all the beneficial owners must be identified. Where such funds are co-mingled at the bank, the bank should still look through to the beneficial owners. Where the banks rely on the 'customer due diligence' (CDD) done by an intermediary, they should satisfy themselves that the intermediary is regulated and supervised and has adequate systems in place to comply

with the KYC requirements. It should be understood that the ultimate responsibility for knowing the customer lies with the bank.

ix. Under the extant AML/CFT framework, therefore, it is not possible for professional intermediaries like Lawyers and Chartered Accountants, etc. who are bound by any client confidentiality that prohibits disclosure of the client details, to hold an account on behalf of their clients. It is reiterated that banks 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.

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

i) Politically exposed persons are individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials, etc. Banks should gather sufficient information on any person/customer of this category intending to establish a relationship and check all the information available on the person in the public domain. Banks should verify the identity of the person and seek information about the sources of funds before accepting the PEP as a customer. The decision to open an account for a PEP should be taken at a senior level which should be clearly spelt out in Customer Acceptance Policy. Banks should also subject such accounts to enhanced monitoring on an ongoing basis. The above norms may also be applied to the accounts of the family members or close relatives of PEPs.

iii) In the event of an existing customer or the beneficial owner of an existing account, subsequently becoming a PEP, banks should obtain senior management approval to continue the business relationship and subject the account to the CDD measures as applicable to the customers of PEP category including enhanced monitoring on an ongoing basis. These instructions are also applicable to accounts where a PEP is the ultimate beneficial owner.

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

99. Accounts of non-face-to-face customers

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

h) Accounts of proprietary concerns

Apart from following the extant guidelines on customer identification procedure as applicable to the proprietor, banks should call for and verify the following documents before opening of accounts in the name of a proprietary concern:

Proof of the name, address and activity of the concern, like registration certificate (in the case of a registered concern), certificate/licence issued by the Municipal authorities under Shop & Establishment Act, sales and income tax returns, CST/VAT certificate, certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities, Licence issued by the Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT, 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 and utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern as required documents for opening of bank accounts of proprietary concerns.

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

104. Procedure to be followed in respect of foreign students:

Banks may follow the following procedure for foreign students studying in India.

107. Banks may open a Non Resident Ordinary (NRO) bank account of a foreign student on the basis of his/her passport (with appropriate visa & immigration endorsement) which contains the proof of identity and address in the home country along with a photograph and a letter offering admission from the educational institution.

108. Within a period of 30 days of opening the account, the foreign student should submit to the branch where the account is opened, a valid address proof giving local address, in the form of a rent agreement or a letter from the educational institution as a proof of living in a facility provided by the educational institution. Banks should not insist on the landlord visiting the branch for verification of rent documents and alternative means of verification of local address may be adopted by banks.

109. During the 30 days period, the account should be operated with a condition of allowing foreign remittances not exceeding USD 1,000 into the account and a cap of monthly withdrawal to Rs. 50,000/-, pending verification of address.

110. On submission of the proof of current address, the account would be treated as a normal NRO account, and will be operated in terms of instructions contained in the Reserve Bank of India's instructions on Non-Resident Ordinary Rupee (NRO) Account, and the provisions of Schedule 3 of FEMA Notification 5/2000 RB dated May 3, 2000.

111. Students with Pakistani nationality will need prior approval of the Reserve Bank for opening the account.

2.6. Selling Third party products

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

113. Even while selling third party products as agents, banks should verify the identity and address of the walk-in customer.

114. Banks should also maintain transaction details with regard to sale of third party products and related records for a period and in the manner prescribed in paragraph 2.24 below.

115. Bank's AML software should be able to capture, generate and analyse alerts for the purpose of filing CTR/STR in respect of transactions relating to third party products with customers including walk-in customers.

116. Sale of third party products by banks as agents to customers, including walk-in customers, for Rs.50,000 and above must be (a) by debit to customers' account or against cheques and (b) obtention & verification of the PAN given by the account based as well as walk-in customers. This instruction would also apply to sale of banks' own products, payment of dues of credit cards/sale and reloading of prepaid/travel cards and any other product for Rs. 50,000/- and above.

2.7. Due Diligence in correspondent banking relationship

Some commercial banks have arrangements with co-operative banks wherein the latter open current accounts with the commercial banks and use the cheque book facility to issue 'at par' cheques to their constituents and walk-in- customers for facilitating their remittances and payments. Since the 'at par' facility offered by commercial banks to co-operative banks is in the nature of correspondent banking arrangements, banks should monitor and review such arrangements to assess the risks including credit risk and reputational risk arising

therefrom. For this purpose, banks 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.

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

In terms of Rule 9 (14)(i) of the PML Rules, simplified norms have been prescribed for those FPIs who have been duly registered in accordance with SEBI guidelines and have undergone the required KYC due diligence/verification prescribed by SEBI through a Custodian/Intermediary regulated by SEBI. Such eligible/registered FPIs may approach a bank for opening a bank account for the purpose of investment under Portfolio Investment Scheme (PIS) for which KYC documents prescribed by the Reserve Bank (as detailed in Annex II of the circular DBOD.AML.BC.No.103/14.01.001/2013-14 dated April 3, 2014) would be required. For this purpose, banks may rely on the KYC verification done by the third party (i.e. the Custodian/SEBI Regulated Intermediary) subject to the conditions laid down in Rule 9 (2) [(a) to (e)] of the Rules.

2.9. Small Accounts

In terms of Government of India, Notification No. 14/2010/F.No.6/2/2007-E.S dated December 16, 2010, (Annex - III a '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.

(a) A 'small account' may be 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:

i) the designated officer of the bank, while opening the small account, certifies 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 bank 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 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 customer shall be established through the production of "officially valid documents"; and

v) 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".

2.10. Officially Valid Documents under Government of India notifications

(a) The notifications further state that job card issued by NREGA duly signed by an officer of the State Government and the letters issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number can now be accepted as an 'Officially Valid Document'.

(b) E-KYC service of Unique Identification Authority of India (UIDAI) may be accepted as a valid process for KYC verification under the PML Rules. The information containing demographic details and photographs made available from UIDAI as a result of e-KYC process may be treated as an 'Officially Valid Document'. However, the individual user has to authorize to UIDAI, by explicit consent, to release her or his identity/address through biometric authentication to the bank branches/business correspondents.

(c) Further, e-Aadhaar downloaded from UIDAI website may be accepted as an officially valid document subject to the following:

i. If the prospective customer knows only his/her Aadhaar number, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in paragraph (b) above.

ii. If the prospective customer carries a copy of the e-Aadhaar downloaded elsewhere, the bank may print the prospective customer's e-Aadhaar letter in the bank directly from the UIDAI portal; or adopt e-KYC procedure as mentioned in paragraph (b) above; or confirm identity and address of the resident through simple authentication service of UIDAI.

2.11. Operation of Bank Accounts & Money Mules

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

b) In a money mule transaction, an individual with 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 may be recruited by a variety of methods, including spam e-mails, advertisements on genuine recruitment web sites, social networking sites, instant messaging and advertisements in newspapers. When caught, these money mules often have their 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.

c) The operations of such mule accounts can be minimised if banks follow the guidelines on opening of accounts and monitoring of transactions contained in this Master Circular. Banks are, therefore, advised to strictly adhere to the guidelines on KYC/AML/CFT issued from time to time and to those relating to periodical updation of customer identification data after the account is opened and also to monitoring of transactions in order to protect themselves and their customers from misuse by such fraudsters.

2.12. Bank No Longer Knows the True Identity

In the circumstances when a bank believes that it would no longer be satisfied that it knows the true identity of the account holder, the bank should also file an STR with FIU-IND.

2.13. Monitoring of Transactions

a) Ongoing monitoring is an essential element of effective KYC procedures. Banks 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. Banks may 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 have to be subjected to intensified monitoring. Every 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) & jewelers should be taken into account by banks to identify suspicious transactions for filing Suspicious Transaction Reports (STRs) to Financial Intelligence Unit- India (FIU-IND). Banks should put in place a system of periodical review of risk categorization of accounts and the need for applying enhanced due diligence measures. Such review of risk categorisation of customers should be carried out at a periodicity of **not less** than once in six months.

b) It has come to our notice that accounts of Multi-level Marketing (MLM) Companies were misused for defrauding public by luring them into depositing their money with the MLM company by promising a high return. Such depositors are assured of high returns and issued post-dated cheques for interest and repayment of principal. So long as money keeps coming into the MLM company's account from new depositors, the cheques are 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. Further, banks 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, the bank should carefully analyse such data and in case they find such unusual operations in accounts, the matter should 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.

c) Banks 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)]

d) 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. It is, however, observed that there are laxities in effective implementation of the Reserve Bank's guidelines in this area, leaving banks vulnerable to operational risk. Banks should, therefore, ensure compliance with the regulatory guidelines on

KYC/AML/CFT both in letter and spirit. Accordingly, banks were advised to complete the process of risk categorization and compiling/updating profiles of all of their existing customers in a time-bound manner, by end-March 2013.

2.14. 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 taking such a decision. Such decisions need to be taken at a reasonably senior level.

2.15. Risk Management

a) The Board of Directors of the bank should ensure that an effective KYC programme is put in place by establishing appropriate procedures and ensuring their effective implementation. It should cover 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. Banks should, in consultation with their boards, devise procedures for creating risk profiles of their existing and new customers, assess risk in dealing with various countries, geographical areas and also the risk of various products, services, transactions, delivery channels, etc. Banks' policies should address effectively managing and mitigating these risks adopting a risk-based approach as discussed in Para 2.3 (d) above.

b) Banks' internal audit and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. As a general rule, the compliance function should provide an independent evaluation of the bank's own policies and procedures, including legal and regulatory requirements. Banks should ensure that their audit machinery is staffed adequately with individuals who are well-versed in such policies and procedures. Concurrent/ Internal Auditors should specifically check and verify the application of KYC procedures at the branches and comment on the lapses observed in this regard. The compliance in this regard should be put up before the Audit Committee of the Board on quarterly intervals.

2.16. Introduction of New Technologies – Credit Cards/Debit Cards/ Smart Cards/Gift Cards

Banks should 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. Many banks are engaged in the business of issuing a

variety of Electronic Cards that are used by customers for buying goods and services, drawing cash from ATMs, and can be used for electronic transfer of funds. Banks are required to ensure full compliance with all KYC/AML/CFT guidelines issued from time to time, in respect of add-on/ supplementary cardholders also. Further, marketing of credit cards is generally done through the services of agents. Banks should ensure that appropriate KYC procedures are duly applied before issuing the cards to the customers. It is also desirable that agents are also subjected to KYC measures.

2.17. Combating Financing of Terrorism

In terms of PMLA Rules, suspicious transaction should include, *inter alia,*

a. 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-Ind 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:

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

   ii) **"1988 Sanctions List",** which is maintained by the 1988 Committee. This list consists of names previously included in Sections A ("Individuals associated with the Taliban") and B ("Entities and other groups and undertakings associated with the Taliban") of the Consolidated List. The

   Updated 1988 Sanctions list is available at http://www.un.org/sc/committees/ 1988/list.shtml

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.

Banks are advised that 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. Full details of accounts bearing resemblance with any of the individuals/entities in the list should immediately be intimated to RBI and FIU-IND.

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

a) 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.

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

c) 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.

d) 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:

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

ii) 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.

iii) Banks shall also send by post, a copy of the communication mentioned in (ii) 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.

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

v) 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.

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

e) **Freezing of financial assets**

i) On receipt of the particulars as mentioned in paragraph d(ii)) above, IS-I Division of MHA would cause a verification to be conducted by the State Police and /or the Central Agencies so as to ensure that the individuals/ entities identified by the banks 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 five working days from the date of receipt of such particulars.

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

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

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

i) 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.

ii) 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.

iii) 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.

iv) Upon receipt of the requests from the UAPA nodal officer of IS-I Division, the list would be forwarded to banks and the procedure as enumerated at paragraphs 2.18[(c), (d) and (e)] shall be followed.

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

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

Any individual or entity, if it has evidence to prove that the freezing of funds, financial assets or economic resources or related services, owned/held by them has been inadvertently frozen, they shall move an application giving the requisite evidence, in writing, to the concerned bank. The banks shall inform and forward a copy of the application together with full details of the asset frozen given by any individual or entity informing of the funds, financial assets or economic resources or related services have been frozen inadvertently, to the nodal officer of IS-I Division of MHA as per the contact details given in paragraph (d)(ii) 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.

h) **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.

2.19. Jurisdictions that do not or insufficiently apply the FATF Recommendations

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, (latest as on June 30, 2014, being our circular DBOD. AML.No.15245/14.01.001/2013-14 dated March 05, 2014) 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 retained and made available to Reserve Bank/other relevant authorities, on request.

2.20. Correspondent Banking and Shell Bank

a) 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. Banks should gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the other bank's management, major business activities, level of AML/CFT compliance, purpose of opening the account, identity of any third party entities that will use the correspondent banking services, and regulatory/supervisory framework in the correspondent's/respondent's country may be of special

relevance. Similarly, banks should try to ascertain from publicly available information whether the other bank has been subject to any money laundering or terrorist financing investigation or regulatory action. While it is desirable that such relationships should be established only with the approval of the Board, in case the Boards of some banks wish to delegate the power to an administrative authority, they may delegate the power to a committee headed by the Chairman/CEO of the bank while laying down clear parameters for approving such relationships. Proposals approved by the Committee should invariably be put up to the Board at its next meeting for post facto approval. The responsibilities of each bank with whom correspondent banking relationship is established should be clearly documented. In the case of payable-through-accounts, the correspondent bank should be satisfied that the respondent bank has verified the identity of the customers having direct access to the accounts and is undertaking ongoing 'due diligence' on them. The correspondent bank should also ensure that the respondent bank is able to provide the relevant customer identification data immediately on request.

b) **Correspondent relationship with a "Shell Bank"**

Banks should refuse to 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. Banks should not enter into relationship with shell banks and before establishing correspondent relationship with any foreign institution, banks should take appropriate measures to satisfy themselves that the foreign respondent institution does not permit its accounts to be used by shell banks. Banks 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.

2.21. Applicability to branches and subsidiaries outside India

The guidelines contained in this master circular shall apply to the branches and majority owned subsidiaries located abroad, especially, in countries which do not or insufficiently apply the FATF Recommendations, to the extent local laws permit. When local applicable laws and regulations prohibit implementation of these guidelines, the same should be brought to the notice of Reserve Bank. In case there is a variance in KYC/AML standards prescribed by the Reserve Bank and the host country regulators, branches/overseas subsidiaries of banks are required to adopt the more stringent regulation of the two.

2.22. 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 rapid and secure method for transferring value from one location to another.

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

i) 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.

ii) 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.

iii) 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.

iv) 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.

b) 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:

1. Cross-border wire transfers

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

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

iii) Where several individual transfers from a single originator are bundled in a batch file for transmission to beneficiaries in another country, they may be exempted from

including full originator information, provided they include the originator's account number or unique reference number as at (ii) above.

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.

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

c) **Exemptions**

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

d) **Role of Ordering, Intermediary and Beneficiary banks**

i) **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.

ii) **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.

iii) **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.

2.23. Designated Director and Principle Officer

a) **Designated Director**

Banks are required to nominate a Director on their Boards 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. The name, designation and address of the Designated Director is to be communicated to the Director, Financial Intelligence Unit – India (FIU-IND).

b) **Principal Officer**

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

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 form time to time. The Principal Officer will also be responsible for timely submission of CTR, STR and reporting of counterfeit notes and all transactions involving receipts by non-profit organisations of value more than Rupees Ten Lakh or its equivalent in foreign currency to FIU-IND.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.

2.24. 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)

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.*

a) 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:

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;

Explanation - Integrally connected cash transactions referred to at (ii) above

The following transactions have taken place in a branch during the month of April 2008:

Date	**Mode**	**Dr (in Rs.)**	**Cr (in Rs.)**	**Balance (in Rs.) BF - 8,00,000.00**
02/04/2008	Cash	5,00,000.00	3,00,000.00	6,00,000.00
07/04/2008	Cash	40,000.00	2,00,000.00	7,60,000.00
08/04/2008	Cash	4,70,000.00	1,00,000.00	3,90,000.00
Monthly		**10,10,000.00**	**6,00,000.00**	

SUMMATION

iii) As per above clarification, the debit transactions in the above example are integrally connected cash transactions because total cash debits during the calendar month exceeds Rs. 10 lakhs

iv) All transactions involving receipts by non-profit organisations of value more than rupees ten lakh 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]

v) 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

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

vii) All the credit transactions in the above example would not be treated as integrally connected, as the sum total of the credit transactions during the month does not exceed Rs.10 lakh and hence credit transaction dated 02, 07 & 08/04/2008 should not be reported by banks.

b) Information to be preserved

Banks are required to 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.

c) Maintenance and Preservation of Records

i) 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, in terms of PML Amemdment Act 2012 notified on February 15, 2013, banks should maintain for at least five years from the date of transaction between the bank and the client, all necessary records of transactions, both domestic or international, which will permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of persons involved in criminal activity.

ii) 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 five years **after the business relationship is ended** as required under Rule 10 of the Rules *ibid***.** The identification records and transaction data should be made available to the competent authorities upon request.

iii) In paragraph 2.13 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.

d) Reporting to Financial Intelligence Unit - India

i) 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 rupees ten lakh or its equivalent in foreign currency to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND,

Financial Intelligence Unit-India,

6th Floor, Hotel Samrat,

Chanakyapuri,

New Delhi -110021

Website - http://fiuindia.gov.in/

Explanation: Government of India Notification dated November 12, 2009- Rule 2 sub-rule (1) clause (ca) defines Non-Profit Organization (NPO). NPO means any entity or organisation that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a company registered under section 25 of the Companies Act, 1956.

ii) The earlier prescribed multiple data files reporting format has been replaced by a new single XML file format. FIU-IND has released a comprehensive reporting format guide to describe

the specifications of prescribed reports to FIU-IND. FIU-IND has also developed a Report Generation Utility and Report Validation Utility to assist reporting entities in the preparation of prescribed reports. The OM issued on Reporting Formats under Project FINnet dated 31st March,2011 by FIU containing all relevant details are available on FIU's website. Banks In this regard, a reference is also invited to circulars DBOD.AML.BC.No.39/14.01.001/2012-13 and DBOD.AML.BC.No.49/14.01.001/2012-13 dated September 7, 2012 and October 11, 2012 respectively. Accordingly, banks should carefully go through all the reporting formats prescribed by FIU-IND. Accordingly, banks should carefully go through all the reporting formats prescribed by FIU-IND.

iii) FIU-IND have placed on their website editable electronic utilities to enable banks to file electronic CTR/STR who are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data base. It is, therefore, advised that in cases of banks, where all the branches are not fully computerized, the Principal Officer of the bank should cull out the transaction details from branches which are not yet computerized and suitably arrange to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on their website http://fiuindia.gov.in

In terms of instructions contained in paragraph 2.3(b) of this Master Circular, banks are required to prepare a profile for each customer based on risk categorisation. Further, vide paragraph 2.13(d), the need for periodical review of risk categorisation has been emphasized. It is, therefore, reiterated that banks, as a part of transaction monitoring mechanism, are required to put in place an appropriate software application to throw alerts when the transactions are inconsistent with risk categorization and updated profile of customers. It is needless to add that a robust software throwing alerts is essential for effective identification and reporting of suspicious transaction.

2.25. Various Reporting Formats

a) **Cash Transaction Report (CTR)**

While detailed instructions for filing all types of reports are given in the instructions part of the related formats, banks 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. Cash transaction reporting by branches to their controlling offices should, therefore, invariably be submitted on monthly basis (not on fortnightly basis) and banks should ensure to submit CTR for every month to FIU-IND within the prescribed time schedule.

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

forgery of valuable security or documents has taken place and may be reported to FIU-IND in plain text form.

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

iv) CTR should contain only the transactions carried out 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 by the Principal Officer of the bank every month in physical form as per the format specified. The summary should be signed by the Principal Officer and submitted to FIU-India.

vi) In case of Cash Transaction Reports (CTR) compiled centrally by banks for the branches having Core Banking Solution (CBS) at their central data centre level, banks may generate centralised Cash Transaction Reports (CTR) in respect of branches under core banking solution at one point for onward transmission to FIU-IND, provided:

a) The CTR is to be generated in the format prescribed by FIU-IND;
b) A copy of the monthly CTR submitted on its behalf to FIU-India is available at the concerned branch for production to auditors/inspectors, when asked for; and
c) The instruction on 'Maintenance of records of transactions'; 'Information to be preserved' and 'Maintenance and Preservation of records' as contained above in this Master Circular at Para 2.24 (a), (b) and (c) respectively are scrupulously followed by the branch.

However, in respect of branches not under CBS, the monthly CTR should continue to be compiled and forwarded by the branch to the Principal Officer for onward transmission to FIU-IND.

b) **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 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.

v) In the context of creating KYC/AML awareness among the staff and for generating alerts for suspicious transactions, banks may consider the indicative list of suspicious activities contained in Annex-E of the 'IBA's

Guidance Note for Banks, January 2012'.

vi) 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.

c) **Non-Profit Organisation**

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

d) **Cross-border Wire Transfer**

Cross-border Wire Transfer Report (CWTR) is required to be filed by 15th of succeeding month for all cross border wire transfers of the value of more than five lakh rupees or its equivalent in foreign currency where either the origin or destination of fund is in India.

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

a) **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.

b) **Employees' Training**

Banks 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

c) **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.

Annex- I

Customer Identification Procedure

Documents that may be obtained from customers

Features	Documents
Accounts of individuals	(i) Passport (ii) PAN card (iii) Voter's Proof of Identity 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 (vii) Identity card (subject to the bank's satisfaction) (viii) Letter from a recognized public authority or public servant verifying the

	identity and residence of the customer to the satisfaction of bank
- Proof of Address	Any one of the documents from the above submitted as proof of identity which contains an address or any of the following: (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the bank) ((vii) A rent agreement indicating the address of the customer

	duly registered with State Government or similar registration authority.
Accounts of companies - Name of the company - Principal place of business - Mailing address of the company - Telephone/Fax Number	(i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv) Copy of PAN allotment letter (v) Copy of the telephone bill
Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners
Accounts of trusts & foundations - Names of trustees, settlors, beneficiaries and signatories - Names and addresses of the founder, the	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlors, beneficiaries and those holding Power

managers/directors and the beneficiaries - Telephone/fax numbers	of Attorney, founders/managers/ directors and their addresses (iv) Resolution of the managing body of the foundation/association (v) Telephone bill
Accounts of Proprietorship Concerns Proof of the name, address and activity of the concern	· Registration certificate (in the case of a registered concern) · Certificate/licence issued by the Municipal authorities under Shop & Establishment Act, · Sales and income tax returns · CST/VAT certificate

	· Certificate/registration document issued by Sales Tax/Service Tax/Professional Tax authorities · Licenceissuedbythe Registering authority like Certificate of Practice issued by Institute of Chartered Accountants of India, Institute of Cost Accountants of India, Institute of Company Secretaries of India, Indian Medical Council, Food and Drug Control Authorities, registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/ Department, etc. Banks may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of the bank account etc. · 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. · Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern. Any two of the above documents would suffice. These documents should be in the name of the proprietary concern.

Annex -II

File No.17015/10/2002-IS-VI

Government of India

Ministry of Home Affairs

Internal Security-I Division

New Delhi, dated 27th August, 2009

ORDER

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

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

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

(a) freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of or at the direction of the individuals or entities Listed in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism;

(b) prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism;

(c) prevent the entry into or the transit through India of individuals Listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism",

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

1."Order" means the Prevention and Suppression of Terrorism (Implementation of Security Council Resolutions) Order, 2007, as may be amended from time to time.

In order to expeditiously and effectively implement the provisions of Section 51A, the following procedures shall be followed:-

Appointment and Communication of details of UAPA nodal officers

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

(i) The UAPA nodal officer for IS-I division would be the Joint Secretary (IS.I), Ministry of Home Affairs. His contact details are 011-23092736(Tel), 011-23092569(Fax) and e-mail.

(ii) The Ministry of External Affairs, Department of Economic Affairs, Foreigners Division of MHA, FIU-IND; and RBI, SEBI, IRDA (hereinafter referred to as Regulators) shall appoint a UAPA nodal officer and communicate the name and contact details to the IS-I Division in MHA.

(iii) The States and UTs should appoint a UAPA nodal officer preferably of the rank of the Principal Secretary/Secretary, Home Department and communicate the name and contact details to the IS-I Division in MHA.

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

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

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

Communication of the list of designated individuals/entities

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

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

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

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

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

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

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

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

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

(iii) The banks, stock exchanges/ depositories, intermediaries regulated by SEBI and insurance companies shall also send by post a copy of the communication mentioned in (ii) above to the UAPA nodal officer of the state/ UT where the account is held and Regulators and FIU-IND, as the case may be.

(iv) In case, the match of any of the customers with the particulars of designated individuals/entities is beyond doubt**,** the banks stock exchanges / depositories, intermediaries regulated by SEBI and insurance companies would prevent designated persons from conducting financial transactions, under intimation to Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No. 011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post should necessarily be conveyed on e-mail.

(v) The banks, stock exchanges/depositories, intermediaries regulated by SEBI and insurance companies shall file a Suspicious Transaction Report (STR) with FIU-IND covering all transactions in the accounts covered by paragraph (ii) above , carried through or attempted, as per the prescribed format.

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

6. In case, the results of the verification indicate that the properties are owned by or held for the benefit of the designated individuals/entities, an order to freeze these assets under section 51A of the UAPA would be issued within 24 hours of such verification and conveyed electronically to the concerned bank branch, depository, branch of insurance company branch under intimation to respective Regulators and FIU-IND. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy thereof to all the Principal Secretary/Secretary, Home Department of the States or UTs, so that any individual or entity may be prohibited from making any funds, financial assets or economic assets or economic resources or related services available for the benefit of the designated individuals/entities or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of IS-I Division of MHA shall also forward a copy of the order under Section 51A, to all Directors General of Police/Commissioners of Police of all states/UTs for initiating action under the provisions of Unlawful Activities (Prevention) Act.

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

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

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

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

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

10. A copy of this reference should be sent to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The particulars apart from being sent by post would necessarily be conveyed on e-mail. MHA may have the verification also conducted by the Central Agencies. This verification would be completed within a maximum of 5 working days.

11. In case, the results of the verification indicate that the particulars match with those of designated individuals/entities, an order under Section 51A of the UAPA would be issued within 24 hours, by the nodal officer of IS-I Division of MHA and conveyed to the concerned Registrar performing the work of registering immovable properties and to FIU-IND under intimation to the concerned UAPA nodal officer of the State/UT.

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

12. Further, the UAPA nodal officer of the State/UT shall cause to monitor the transactions/accounts of the designated individual/entity so as to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the schedule to the order or any other person engaged in or suspected to be engaged in terrorism. The UAPA nodal officer of the State/UT shall upon coming to his notice, transactions and attempts by third party immediately bring to the notice of the DGP/Commissioner of Police of the State/UT for also initiating action under the provisions of Unlawful Activities (Prevention) Act.

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

13. U.N. Security Council Resolution 1373 obligates countries to freeze without delay the funds or other assets of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the

commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds or other assets derived or generated from property owned or controlled, directly or indirectly, by such persons and associated persons and entities. Each individual country has the authority to designate the persons and entities that should have their funds or other assets frozen. Additionally, to ensure that effective cooperation is developed among countries, countries should examine and give effect to, if appropriate, the actions initiated under the freezing mechanisms of other countries.

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

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

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

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

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

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

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

19. The Joint Secretary (IS-I), MHA, being the nodal officer for (IS-I) Division of MHA, shall cause such verification as may be required on the basis of the evidence furnished by the individual/entity and if he is satisfied, he shall pass an order, within 15 working days, unfreezing the funds, financial assets or economic resources or related services, owned/held by such applicant under intimation to the concerned bank, stock exchanges/depositories, intermediaries regulated by SEBI, insurance company and the nodal officers of States/UTs. However, if it is not possible for any reason to pass an order unfreezing the assets within fifteen working days, the nodal officer of IS-I Division shall inform the applicant.

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

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

Regarding prevention of entry into or transit through India

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

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

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

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

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

(D .Diptivilasa)

Joint Secretary to Government of India

Annex - III

Government of India

Ministry of Finance

(Department of Revenue)

Notification

New Delhi, the 16th December 2010

GSR ------ (E) – In exercise of the powers conferred by sub-section (1) read with clauses (h) (i), (j) and (k) of sub-section (2) of Section 73 of the Prevention of Money-laundering Act, 2002 (15 of 2003), the Central Government hereby makes the following amendments to the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Rules, 2005, namely::-

1. (1)These rules may be called the Prevention of Money- laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking Companies, Financial Institutions and Intermediaries) Third Amendment Rules, 2010.
(2) They shall come into force on the date of their publication in the Official Gazette.

2. In the Prevention of Money-laundering (Maintenance of Records of the Nature and Value of Transactions, the Procedure and Manner of Maintaining and Time for Furnishing Information and Verification and Maintenance of Records of the Identity of the Clients of the Banking

Companies, Financial Institutions and Intermediaries) Rules, 2005, -

(a) in rule 2,-

(i) after clause (b), the following clause shall be inserted, namely:- "(bb) "Designated Officer" means any officer or a class of officers authorized by a banking company, either by name or by designation, for the purpose of opening small accounts".

(ii) in clause (d), for the words "the Election Commission of India or any other document as may be required by the banking company or financial institution or intermediary", the words "Election Commission of India, job card issued by NREGA duly signed by an officer of the State Government, the letter issued by the Unique Identification Authority of India containing details of name, address and Aadhaar number or any other document as notified by the Central Government in consultation with the Reserve Bank of India or any other document as may be required by the banking companies, or financial institution or intermediary" shall be substituted;

(iii) after clause (fa), the following clause shall be inserted, namely:-

"(fb) "small account" means a savings account in a banking company where-

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

(b) In rule 9, after sub-rule (2), the following sub-rule shall be inserted, namely:-

"(2A) Notwithstanding anything contained in sub-rule (2), an individual who desires to open a small account in a banking company may be allowed to open such an account on production of a self-attested photograph and affixation of signature or thumb print, as the case may be, on the form for opening the account.

Provided that –

(i) the designated officer of the banking company, while opening the small account, certifies 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, as referred to in sub rule (2) of rule 9"; and
(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, as referred to in sub-rule (2) of rule 9."

(Notification No.14/2010/F.No.6/2/2007-ES)

(S.R. Meena)

Under Secretary

GLOSSARY OF TERMS

AML Anti-Money Laundering
BM Branch Manager
BDD Basic Due Diligence
CAP Customer Acceptance Program
CBI Central Bureau of Investigation
CBS Core Banking Solution
CCR Counterfeit Currency Report
CRCM Customer Risk Categorisation Model
CDD Customer Due Diligence

CIP Customer Identification Program
CRO Customer Relationship Officer
CTR Cash Transaction Report
DCCB District Central Cooperative Bank
EDD Enhanced Due Diligence
FATF Financial Action Task Force
FIU-IND Financial Intelligence Unit - India
HNI High Net Worth Individual
HUF Hindu Undivided Family
IBA Indian Banks' Association
KYC Know Your Customer
ML Money Laundering
NRI Non-Resident Indian
PACS Primary Agricultural Cooperative Societies
PEP Politically Exposed Person
PIO Person of Indian Origin
PMLA Prevention of Money Laundering Act 2002
PMLR Prevention of Money Laundering Rules 2005
PO Principal Officer
RBI Reserve Bank of India
RRB Regional Rural Banks
NABARD National Bank for Agriculture and Rural Development
NAFSCOB National Federation of State Cooperative Banks
NRI Non Resident Indian
NSDL National Securities Depository Limited
NTR Non-Profit Organisation Transaction Reports
SA Staff Assistant
SCB State Cooperative Banks
SDD Simplified Due Diligence
STR Suspicious Transaction Report
UAPA Unlawful Activities Prevention Act
UN United Nations
UNSCR United Nation Security Council Resolution

Aml kyc recollected questions 1st of September 2018
3 steps of basic money laundering cycle
2 questions on funnel accounts
Connected accounts
1 question on wire transfer
1 question on hawala
Non member of Wolfsburg group
Law in UK related to AML
Around 5 questions on 2017 amendments of pmla (already discussed here in this group)

1 question on NI act
1 question on intermediates (non-intermediaries of options)
1 question on whether to file STR
1 question on who will decide to file STR
Time limit for STR
1 question on enhanced due diligence
Time limit for freezing accounts
Time limit for kyc updation
1 question on juridical persons
1 question on specific beneficial owner
1 question on small account
1 question on cross border wire transfer
CTR time limit for filling
Which report don't have ceiling limits
STR typology
Staff callousness
Principal officer
Kyc aml interconnectedness

6 oct 2018 12:30pm aml recollected que-
1. Meaning of money laundering.
2. India is member of which group?
3. Funnel account-case study
4. Structuring-case study & 1que
5. Back to back loan-case study
6. Difference between ML & TF
7. Placement & layering- 2case study & 1que
8.For beneficial owner determination min percent in company, proprietory firm, trust - 3 que
9. Suspicious txn. report -1case study & 2que
10. Fiu-Ind help which country for technical assistance?
11. Us sanction list
12. Law related to UK-2que
13. Fatf 4th round evaluation-3que
14. Limit for CDD in case cross border txn

15. Authority for prosecution in case TF
16. Fatf public statement how many times in a year
17. Limit of account opened by OTP
18. PMLA latest amendments 2017- 5que
19. Comprehensive que regarding FATF recommendation 4 que(Sug-plz study carefully)
20. CDD for PEP
21. CDD Procedure & guideline for opening account as per BCBS paper
22. Within how many days records are sent to Central kyc regustry
23. Reports r sent to 15th of the month
24. STR is sent to how many days
25. Which bank is not a member of wolfsgrp?
26. Difference between FATF, EGMONT GROUP, WOLFSBERG & BSBS
27. Purpose of FATF
28. Direct que from FATF recommendation relating to PEP, NPO, Correspondent banking, Money or value transfer services -4que
29. CDD not required for which DNFBP
30. CDD for juridical person and their firm-2que
31. Main feature of Vienna convention
32. Who is authorised to take prosecution under PMLA-ED
33. Authorised to seize property under UAPA-NIA
34. Max penalty for non-compliance of kyc-100000
35. Punitive action for non-compliance under PMLA
36. Reporting entity means
37. Conterfeit currency reporty is submitted monthly
38. All reports are sent 15th
39. FATF identified countries -3que
40. Key elememt of KYC policy
41. Purpose of FAQ
42. Kyc policy is approved by
43. The five major factors that impact ML/TF
44. Foreign student account
45. Money laundering risk relating to new products/new technology
46. Easy method for terrorist financing
47. One case study relating to TF through trust
48. One case study regarding what should be kyc risk category for salaried person if get inward cross-border remmitance
49. Risk involved in third party business
50. If ovd does not contain address then Which utility bill required

51. What contain in Due diligence & transparency regarding cover payment message related to cross border wire transfer

Recollected qns of kyc and aml- 23/03/2019
1. CBTR Is to be submitted- 15 th of every month.
2. Designated director- criteria
3. Str typology- benami entity/mlm activity
4.placement- one qn
5. Integration
6. CKYC R - reporting entity
7. Small account-the aggregate of all withdrawals and transfers in a month does not exceed rupees ten thousand
8. Funnel account
9.hawala system
10.CDD- fill form
11. UCIC - fullform
12. If SHG is opening SB account- kyc details is obtained for all members or few
13.can NRI student wants to open his SB account with introduction letter from principal
14.walk in customer has to provide kyc documents if amount involved is rs 50000 or more
15.4 to 5 qns from STR...
16.correspondant banking- regulatory actions and due diligence
17 .FATF- which is regional body among options
18. Egmont group- informal network of fiu
19. Fiu is responsible for
20. Terrorism comes under which - ministry of defense/ finance minister or govt
21. Staff training
22.money laundering
23. UAPA
24. SIFO is set up under ministry of corporate affairs
25. If customer comes for opening account - ekyc of customer has to be captured
26. Passport as ovd is for- only nri/ only nro/ only if is issued under regional officer/

27. Risk categorisation

28.proprietary firm account can be opened which ovd among options.

29. PEP

30. Staff callousness- staff should not disclose banks policy and procedures with outsiders

31. Staff training should not be given to senior MGMT/designated director/ board of directors/ shareholders

32. One qn on audit

33.Questions also on role of senior management, ekyc, vostro account,

Disclaimer

While every effort has been made by me to avoid errors or omissions in this publication, any error ordiscrepancy noted may be brought to my notice throughr e-mail to Srinivaskante4u@gmail.com which shall be taken care of in the subsequent editions. It is also suggested that toclarify any doubt colleagues should cross-check the facts, laws and contents of this publication with original Govt. / RBI / Manuals/Circulars/Notifications/Memo/Spl Comm. of our bank.