AML KYC GUIDELINES

CHAPTER 2 MODULE A PPB By Ashish Sir

Stages of Money Laundering

Money laundering is the process of making illegally obtained money appear legitimate. It typically involves three stages:

1. **Placement**:

- The first step where illicit money enters the financial system.
- Techniques include:
  - Depositing cash into bank accounts.
  - Breaking large amounts into smaller deposits (structuring or smurfing).
  - Using cash to purchase assets (e.g., real estate, luxury items).
- **Objective**: To avoid detection and place "dirty money" into legitimate circulation.

2. **Layering**:

- The process of concealing the illicit origin of the money through a complex series of financial transactions.

- Techniques include:
  - Transferring funds across multiple accounts and jurisdictions.
  - Using shell companies or offshore accounts.
  - Investing in financial instruments or high-value goods.
- **Objective**: To obscure the money's trail and make it hard to trace.

3. **Integration**:

- The final step where laundered money is fully integrated into the legitimate economy.
- Techniques include:
  - Investing in businesses or real estate.
  - Using funds to acquire legitimate assets or luxury goods.
  - Declaring money as legitimate business income.
- **Objective**: To make the funds appear legally earned and usable without suspicion.

placement Layering Integration

AML → ML

CFT → FT

Imp

Stages of Financing Terrorism

1. **Raising**: Funds are collected through legal (e.g., donations, charities) or illegal (e.g., smuggling, drug trafficking) means.
2. **Moving**: Funds are transferred using methods like hawala networks, banking systems, or cash smuggling to avoid detection.
3. **Storing**: Funds are held in cash reserves, bank accounts, or assets, ensuring availability when required.
4. **Using**: Funds are deployed for operational purposes such as procuring weapons, logistics, recruitment, or propaganda.

#4

#3

#2

#1

Aspect	Money Laundering	Terror Financing
Objective	Conceal the origin of illicit funds.	Support terrorist activities.
Source of Funds	Proceeds from criminal activities.	Can come from legal (donations) or illegal sources.

Focus	Making dirty money appear clean.	Ensuring funds reach and are used for terrorist acts.
Legal Framework	Anti-Money Laundering (AML) laws.	Counter-Terrorism Financing (CTF) laws.

Objectives of Prevention of Money Laundering

1. **Protect the Integrity of Financial Systems**: Ensure financial institutions are not misused for laundering illicit funds.
2. **Combat Financial Crimes**: Disrupt criminal enterprises by cutting off access to illicit proceeds.
3. **Prevent Terrorism Financing**: Block funds that support terrorist organizations and activities.
4. **Enhance Legal and Regulatory Compliance**: Enforce domestic and international anti-money laundering laws.
5. **Promote Economic Stability**: Prevent market distortions caused by laundered money.
6. **Safeguard National Security**: Protect against financial empowerment of criminal and terrorist entities.
7. **Encourage Ethical Business Practices**: Foster compliance and accountability in businesses and financial institutions.

8. **Facilitate Cross-Border Cooperation**: Strengthen international collaboration to combat global money laundering.
9. **Promote Financial Inclusion**: Build trust in financial systems to encourage broader participation.
10. **Deter Future Criminal Activities**: Enforce penalties and seize illicit gains to discourage money laundering.

Legal Framework for Money Laundering in India

1. **Enactment of PMLA, 2002**:
   - Based on FATF (Financial Action Task Force) recommendations.
   - Covers financial and non-financial businesses (designated as **Reporting Entities (RE)**).
   - Legal obligations for REs detailed in the **Prevention of Money Laundering (Maintenance of Records) Rules (PMLR)**.
   - Institutional framework established for combating money laundering crimes.

Money Laundering Offence

- **Definition** (Section 3, PMLA):

  - Engaging directly or indirectly in activities involving proceeds of a crime, including concealment, possession, acquisition, or projection as untainted property, constitutes the offence of money laundering.
- **Cognizable and Non-Bailable**:
  - Section 45: Money laundering offences are deemed **cognizable** and **non-bailable**.
- **Punishment** (Section 4):
  - **Rigorous imprisonment**:
    - Minimum: 3 years.
    - Maximum: 7 years (extendable to 10 years for offences under the **Narcotics Drugs and Psychotropic Substances Act**).
  - **Fine**: Based on the gravity of the offence.

Money Laundering - Risk Perception

- Criminals exploit financial products for laundering money and financing terrorism by masking identities and activities.
- Example: A gambling operator disguises betting money inflows by posing as a freelancer.

Risk Factors:

1. **Customer Profile**: True identities, purposes, and profiles of customers may be misrepresented.
2. **Other Influencing Factors**:

- Nature of financial products and services.
- Country of bank incorporation.
- Location of the bank branch and connected transactions.
- Nature and value of transactions.

Measures to Mitigate Money Laundering Risk

1. **Obligations Under PMLA**:

Banks must: CDD

- Understand customers and their financial activities.
- Detect and report suspicious activities to **FIU-Ind**.
- Comply with laws and regulations.
- Train staff on KYC/AML procedures.

2. **Key Measures**: Mitigate risks by monitoring activities and discouraging criminal abuse of financial services.
3. **Institutional Framework**:

FIU-Ind: financial intelligence unit India

- Receives and analyzes financial transaction reports.
- Supervises entities subject to PMLA.

Enforcement Directorate (ED):

- Investigates and prosecutes money laundering crimes.
- Tracks and attaches assets related to offences.

Special Courts:

- Adjudicate money laundering cases.
- Freeze and confiscate assets linked to laundering.

Regulators: Issue operating guidelines for compliance with PMLA and PMLR.

Organizational Set-Up for Anti-Money Laundering (AML)

Under the **Prevention of Money Laundering (Maintenance of Records) Rules, 2005 (PMLR)**, banks are required to establish a robust organizational structure to fulfill Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) obligations. Key roles and responsibilities are designated to ensure compliance with the **Prevention of Money Laundering Act, 2002 (PMLA)**.

Key Roles in AML Organizational Set-Up

1. **Designated Director (DD):**

FS
A
DD

Responsibilities:

- Ensures the bank's overall compliance with PMLA, PMLR, and regulatory guidelines.

- Supervises the establishment of systems and processes for KYC/AML compliance.
- Maintains an updated KYC Policy.
- Ensures staff are skilled and capable of handling AML/CFT tasks.
- Adapts measures to address changing risks related to Money Laundering (ML) and Terrorist Financing (TF).

Designation Requirements:

- For companies: Managing Director or Whole-Time Director, authorized by the Board.
- For partnerships: Managing Partner.
- For proprietorships: Proprietor.
- For trusts: Managing Trustee.
- For unincorporated associations: Individual managing its affairs.
- For cooperative or rural banks: Senior management personnel.

1 DD
2 PO

2. **Principal Officer (PO)**:

- **Primary Role**:
    - Acts as the **Money Laundering Reporting Officer (MLRO)**.

- **Functions**:
  - Oversees the implementation of the bank's KYC/AML Policy.
  - Reports financial transactions to **Financial Intelligence Unit-India (FIU-Ind)**.
  - Liaises with law enforcement agencies for AML-related matters.
  - Submits regular reports to the Board or top management.
  - Ensures that AML monitoring systems remain up-to-date.

- A dedicated team tasked with ensuring compliance with AML and CFT regulations.
- **Key Functions**:
  - Regularly updates the bank's KYC Policy.
  - Assists business and operations units with customer identification and due diligence processes.
  - Conducts risk assessments for ML/TF and reviews them periodically.

DD
PO
AML Team

- Guides operational units in customer risk categorization.
- Monitors transactions to detect and flag suspicious activities.
- Submits prescribed reports and provides information requested by FIU-Ind.

Core Responsibilities Across Units

- **System Set-Up**: Establish appropriate systems, processes, and functional set-ups for KYC/AML.
- **Staff Competence**: Ensure all levels of staff are trained and equipped to manage AML responsibilities.
- **Proactive Adaptation**: Take measures to address evolving ML/TF risks effectively.

Obligations Under the Prevention of Money Laundering Act (PMLA)

The **Prevention of Money Laundering Act, 2002 (PMLA)**, mandates the following obligations for **Reporting Entities (REs)**, including banks:

1. **Customer Identification and Verification**:

- Verify the identity of customers and their **beneficial owners** using specified modes:
  - **Aadhaar authentication** (online or offline), **passport**, or any officially valid documents.

2. **Transaction Record Maintenance**:
   - Maintain records of all transactions, including:
     - Completed transactions.
     - **Attempted transactions** (whether successful or not).
   - Retain these records for **5 years** from the transaction date.

3. **Identity and Correspondence Record Maintenance**:
   - Preserve records of:
     - Identity documents of clients and beneficial owners.
     - Account files and business correspondence.
   - These records must be retained for **5 years** from:
     - The **closure of the account**, or
     - The **end of the business relationship**, whichever is later.

4. **Confidentiality**:

- Ensure that all maintained and furnished information remains **confidential**.

5. **Verification Before Commencing Transactions**:
   - Before executing specified transactions, banks must:
     - **Verify client identity** through Aadhaar or other prescribed modes.
     - Examine:
       - **Ownership structure** of the customer.
       - **Financial position** and **source of funds**.
     - Record:
       - **Purpose of the transaction**.
       - **Nature of the relationship** between the transaction parties.
   - Specified transactions include:
     - Cash withdrawals/deposits above thresholds.
     - Foreign exchange transactions exceeding limits.
     - High-value imports and remittances.
     - Transactions linked to **money laundering** (ML) or **terrorist financing** (TF) risks.

6. **Prohibition on Transactions Without Compliance**: Do not proceed with any specified transaction unless the above measures are taken.

7. **Enhanced Monitoring for Suspicious Transactions**:
    - If a transaction is deemed suspicious:
        - Apply **enhanced monitoring** to the relationship.
        - Conduct greater scrutiny of such transactions.

Significance

These obligations aim to:

- Prevent misuse of banking and financial systems for money laundering and terrorist financing.
- Ensure robust compliance and regulatory oversight to mitigate ML/TF risks effectively.

RISK MANAGEMNT

RBA/RA/

1. Adoption of Risk-Based Approach (RBA)

- Banks must:
    - Apply RBA to mitigate and manage identified risks effectively.

  - Develop **Board-approved policies**, controls, and procedures.
  - Regularly monitor and enhance these controls as necessary.

RBA

- **Objective**:
  - Tailor customer due diligence and transaction monitoring to risk levels.
  - Ensure effective implementation of AML/CFT measures.

2. Risk Assessment

- Banks should assess risks stemming from:
  - **Customers**.
  - **Products/Services** offered.
  - **Regions/Countries** of operation.
  - **Delivery channels**.
  - **Customer transactions**.

FD/RD — CBWT

- Assessment should:
  - Align with the bank's size, structure, geographical presence, and complexity.
  - Be conducted **at least annually**.

HR 2Y
LR 10Y

3. Customer Risk Categorization

- Customers are classified into three categories based on risk perception:
  - **High Risk**: Includes customers like **Politically Exposed Persons (PEPs)** and others needing heightened monitoring.
  - **Medium Risk**.
  - **Low Risk**.
- **Risk Parameters**:
  - Nature of business activity.
  - Customer's location and clientele.
  - Payment modes, turnover, and social/financial status.
- **Periodic Review**:
  - Risk categorization reviewed **every six months**.
  - Adjusted based on new information or changes in customer behavior.

4. Role of Other Functions

- **Management Oversight**:
  - Framework for oversight, controls, and related procedures.
- **Internal Audit**:

- Independent evaluation of KYC/AML compliance.
- Verification of KYC/AML procedures at branch level.
- Findings presented quarterly to the **Audit Committee of the Board**.

5. Introduction of New Technologies

- Emerging technologies like **mobile wallets**, **RTGS**, **NEFT**, etc., may introduce new risks.
- Banks must:
  - Integrate **appropriate KYC procedures** before launching new products/services.

6. Staff Hiring and Training

Screening:

- Implement robust mechanisms during recruitment to mitigate risks posed by staff roles and access.
- Conduct due diligence on third parties (e.g., Business Correspondents, Recovery Agents).

Training:

- **Role-based training** to ensure understanding of AML/CFT responsibilities.
- Ongoing training to update staff on regulatory changes and emerging criminal modalities.