

MONEY LAUNDERING SOME METHODS




CH – 2 KYC/AML PART A


2.1.1 Nature of the Money Laundering Process

 Money laundering is complex & constantly evolving  


 Criminals use financial institutions at multiple stages  










 Depends on:




- Source & amount of illegal funds 
- Geographic scope 
- Sophistication of techniques 

 **Example:** A drug dealer deposits cash into **multiple bank accounts** to avoid suspicion, then transfers it to offshore entities.

2.1.2 Basic Money Laundering Cycle

 Three stages of money laundering:

 Stage	 Description	 Banking Risk
  	Depositing illicit funds into financial system	Large cash deposits, multiple accounts
  	Obscuring origins by complex transactions	Multiple fund transfers, offshore transactions

  	Converting into legal assets (stocks, real estate)	Difficult to track, appears legitimate
--	--	--

📌 **Example:** A corrupt politician places bribes into **shell companies** (placement), moves funds across borders (layering), and buys luxury hotels (integration).

📌 2.1.2.1 Placement – Entering Dirty Money into Banking

✅ First stage – introducing illicit funds into banks

✅ Methods Used:

- Multiple small cash deposits to avoid detection 💰 🏦
- Cash smuggling across borders ✈️ 🧳
- Using casinos, betting, or cash-based businesses 🎰 🕒

🚨 How Banks Can Detect?

🔍 Large/unusual cash deposits 🏦 💰

🔍 Frequent transactions just below reporting limits (₹49,000 instead of ₹50,000)

🔍 Customers reluctant to provide KYC details 🆔 ❌

📌 **Example:** A human trafficker deposits cash from victims' ransoms into **multiple small accounts** to avoid scrutiny.

📌 2.1.2.2 Layering – Concealing the Source

✅ Second stage – disguising the origin of money

✅ Methods Used:

- Multiple fund transfers across accounts & countries 🌐 💳
- Fake invoices for imports/exports 📄 🚢
- Shell companies & offshore accounts 🌴 🏢
- Cryptocurrency conversions ₿ 💻

🚨 How Banks Can Detect?

🔍 Frequent international transfers with no clear business purpose



🔍 High-value transactions from unknown sources 💰 ⚠️

🔍 Unusual investments in art, jewelry, or real estate 🖼️ 🏠

📌 **Example:** A fraudster routes money through five countries using offshore bank accounts, making it difficult to track.

📌 2.1.2.3 Integration – Converting to "Clean" Money

✅ Final stage – re-entering money into the legal economy

✅ Methods Used:

- Real estate purchases (luxury properties, hotels, malls) 🏢 🏠
- Stock market investments & mutual funds 📈 📈



- High-end business ventures (construction, film production, cryptocurrency mining) 🎬 ⚒️

🚨 How Banks Can Detect?

- 🔍 High-value purchases with no clear income source 🏛️ 💳
- 🔍 Frequent large cash withdrawals after multiple deposits 💰 📄
- 🔍 Companies with no real business activity making huge profits 📄 🔍

📌 **Example:** A smuggler buys high-value paintings & jewelry to later resell as “clean” money.

📌 2.1.3 Lessons for Bankers: How to Detect Money Laundering?

 Money Laundering Stage	 Bank Detection Measures
Placement 💰 📄	Monitor large cash deposits, multiple small deposits, structured transactions
Layering 🔄 💳	Flag rapid fund transfers, offshore accounts, mismatched business transactions
Integration 🏛️ 📈	Watch for luxury purchases, large investments, unknown business sources

📌 Why Is This Important?

- ✅ Protects **bank reputation** 🏛️ 🛡️

✓ Ensures compliance with AML laws 📄 ⚖️

✓ Prevents severe financial penalties 💰 🚨

📌 **Example:** In 2018, Deutsche Bank was fined \$630 million for failing to detect Russian money laundering transactions.

🏛️ **Final Summary** 🖋️

💡 Money laundering follows a 3-step process – Placement,

Layering, Integration 📥 🔄 📈

💡 Criminals use banks, shell companies, real estate, and cryptocurrencies 🏛️ 🏢 💰

💡 Banks must monitor transactions, KYC compliance, and suspicious activities 🔍 ⚖️

💡 Failure to detect money laundering can result in huge fines & reputational damage 🚨 🏛️

📌 **A strong AML (Anti-Money Laundering) framework is key to preventing financial crimes!** 🚀

Would you like MCQs, case studies, or practical banking compliance insights for JAIIB/CAIIB? 📖 🏛️ 😊

🏛️ **Terrorism Financing & Common Sources of Illegal Money** 💰 🚨

📌 2.2 Terrorism Financing: An Overview

✅ Terrorism financing refers to mobilizing funds for supporting terrorist acts or organizations 🚬💰

✅ Funds can come from both legal & illegal sources 📄🔍

✅ Unlike money laundering, terrorist financing hides the purpose of funds, not their origin 🤫💳

📌 **Example:** A fake NGO collects donations for "education" but secretly funds a terrorist group.

📌 2.2.1 Features of Terrorism Financing

◆ **Two Key Dimensions:**

🔍 Type	🎯 Purpose	💰 Fund Movement
Specific Terrorist Acts 🎯	Bombings, assassinations, attacks 🚬	Low-value transactions disguised as remittances
Terrorist Organizations 🏛️	Recruitment, training, propaganda, logistics	Large-scale, cross-border funding

✅ Terrorist groups disguise funds as donations, social welfare, medical aid, etc. 🏥📄

📌 **Example:** A charity in one country raises money for "war relief" but sends it to terrorist training camps.

📌 2.2.2 Financing of Terrorist Acts

✅ **Individual terrorist acts require small amounts of money** 💰 📌

✅ **Funds are transferred as:**

- Personal remittances 🏠 📌
- Business transactions 🏢 📄
- Charitable contributions 🙌 💰

📌 **Why Is It Hard to Detect?**

- Transactions are **low-value** and often appear normal 💰 🔍
- **Innocent people** are used as fund couriers unknowingly 🚶 🏠

📌 **Example:** A person receives a small bank transfer from abroad for "family support" but unknowingly passes the funds to a terrorist handler.

📌 2.2.3 Financing of Terrorist Organizations

✅ **Terrorist organizations require long-term financial support**



🔍 **Three Key Sources of Funding:**

 Source	 Description	 Examples
---	--	---

JAIIB/ CAIIB/ PROMOTIONS/ CERTIFICATIONS Course available

<https://iibf.info/iibfLearning>

1 State Sponsorship 🏛️	Governments provide funding for covert terrorist groups	Grants, subsidies, diplomatic funds
2 Legitimate Channels ✅	Donations, charities, businesses	Crowdfunding, religious institutions
3 Criminal Activities ❌	Illegal sources of money	Drug trafficking, kidnappings, extortion



📌 **Example:** A terrorist organization runs a "**charitable school**" but secretly trains militants & receives government-backed funding.

📌 2.2.4 Lessons for Bankers: Detecting Terrorist Financing

✅ **Challenges:**




- Terrorist transactions are **small in value** 💰 🔍
- **Difficult to distinguish between real & fake charities** 🏛️ 📄
- Many transactions occur in **high-risk locations** 🌍


📌 **How Banks Can Detect Suspicious Transactions?**

🔍 Red Flag	⚠️ Suspicious Activity
Frequent low-value remittances  	Structuring transactions to avoid detection

JAIIB/ CAIIB/ PROMOTIONS/ CERTIFICATIONS Course available

<https://iibf.info/iibfLearning>








Unusual donations to charities 	Charity with no clear operations
Cash deposits from multiple sources 	Funds collected for undisclosed purposes
Transfers to conflict zones 	Wire transfers to sanctioned regions

 **Example:** A terrorist group receives **small donations from hundreds of accounts** to finance operations without raising alarms.

2.3 Common Sources of Illegal Money

 **Criminals generate illegal money through:**

2.3.1 Typical Criminal Activities

 Crime Type	 Description
Drug Trafficking 	Cocaine, heroin smuggling
Organized Crime 	Extortion, contract killings, loan sharking
Illegal Arms Trade 	Cross-border weapons sales
Human Trafficking 	Smuggling & forced labor
Smuggling 	Illegal goods, fake currency

Corporate Bribery

Slush funds, corruption




Bank Fraud 

Loan scams, counterfeit money

📌 **Example:** A smuggler hides **drug profits in real estate investments** to avoid detection.

📌 2.3.2 Tax Evasion & Money Laundering

✅ **Why Is Tax Evasion a Concern?**

- Uses **similar laundering techniques** 
- Hard to detect due to **offshore accounts** 
- Many countries **do not classify tax evasion as a crime** ❌ 

📌 **Example:** A businessman **hides undeclared income in Swiss bank accounts** to avoid taxes.

 **Methods & Techniques of Money Laundering & Terrorism**

Financing 

📌 2.4 Overview of Money Laundering & Terrorism Financing

Methods

✅ **Criminals use banks & financial systems to move illicit funds**



JAIIB/ CAIIB/ PROMOTIONS/ CERTIFICATIONS Course available

<https://iibf.info/iibfLearning>

✓ Techniques aim to disguise the origin or purpose of money



✓ Common methods involve deposits, transfers, fake businesses

& offshore accounts 🌐 🌴

📌 **Example:** A drug cartel launders money through **multiple small bank deposits** (smurfing), then wires funds to **offshore accounts** before buying **luxury real estate**.

📌 2.4.1 Using Normal Banking Services 🏦 💰

🔍 2.4.1.1 Deposit Structuring (Smurfing)

✓ Breaking large deposits into small amounts below reporting limits 📉 💰

✓ Multiple accounts & unconnected depositors used 🏦 🔍

📌 **Example:** A criminal deposits ₹9.9 lakh in different accounts to avoid the ₹10 lakh reporting limit.

🚨 **Red Flags for Banks:**

- Frequent small deposits just below reporting thresholds 🔍
- Multiple individuals depositing into one account 🏦

2.4.1.2 Multiple Tiers of Accounts

 Funds are split & transferred through multiple accounts  

 Creates a complex transaction trail making detection difficult

 **Example:** A fraudster moves ₹1 crore through 20 accounts, splitting it into ₹5 lakh per account.


Red Flags:

- Multiple small transactions leading to large final transfers
- Frequent intra-bank or cross-border transfers

2.4.1.3 Funnel Accounts

 Deposits made in one location & withdrawn in another  

 Used by organized crime & terror groups

 **Example:** A fake business collects cash deposits in Mumbai and withdraws funds in Dubai within hours.

Red Flags:

- Frequent deposits from multiple sources, followed by immediate withdrawals
- High-volume transactions without business justification

2.4.1.4 Contra Transactions

 Back-and-forth transactions between accounts to inflate

turnover  




 Creates the illusion of legitimate business activity

 **Example:** A company transfers ₹50 lakh between accounts daily to appear financially strong.


 **Red Flags:**

- High-volume transactions with no real business purpose
- Funds move between accounts without being used

2.4.1.5 Bank Drafts & Similar Instruments

 Cash is used to buy bank drafts or money orders to avoid detection  

 Makes tracking illicit funds harder for authorities

 **Example:** A fraudster buys ₹10 lakh in demand drafts & deposits them overseas.

 **Red Flags:**


- Frequent purchase of high-value drafts or cashier's checks
- Use of multiple instruments to move money abroad

2.4.1.6 Cash Deposits Followed by Transfers

 Large cash deposits immediately wired to another account






 Common in drug trafficking & tax evasion

 **Example:** A smuggler deposits ₹50 lakh in India & transfers it to Hong Kong as "business payments".


 **Red Flags:**

- Frequent large cash deposits followed by quick transfers
- Transactions with no clear business purpose

2.4.1.7 Connected (Benami) Accounts

 Accounts in relatives' or associates' names used to hide ownership  

 Often operated by lawyers or shell companies

 **Example:** A corrupt politician launders ₹10 crore through family members' accounts.

 **Red Flags:**

- Unusual fund movements between linked accounts
- Transactions inconsistent with account holder's profile

2.4.1.8 Front Companies

✓ Fake or high-cash businesses used to mix illicit funds with

legitimate earnings  

✓ Casinos, restaurants & real estate firms commonly used

📌 **Example:** A drug cartel buys a hotel & launders cash as "room bookings".

 **Red Flags:**

- High cash deposits with no clear business explanation
- Business with no real customer base but high revenue

2.4.1.9 Legitimate Accounts (Money Mules)

✓ Using genuine bank accounts for laundering  

✓ Owners unaware or paid a small fee

📌 **Example:** A student lends his account to a fraudster for "temporary transactions".


 **Red Flags:**


- Unexpected large deposits in a personal account
- Account holder unable to explain transactions

2.4.1.10 Dormant Accounts

 Old or inactive accounts reactivated for money laundering





 Terrorists use them for receiving funds without drawing attention

 **Example:** A terrorist group reactivates an old account to fund attacks.


 **Red Flags:**

- Large transfers into recently reactivated accounts
- Frequent withdrawals in small amounts to avoid suspicion

2.4.1.11 Wire Transfers

 International transfers used for moving illicit funds  

 Preferred by money launderers for cross-border transactions


 **Example:** A scammer wires ₹5 crore to an offshore bank in Cayman Islands.


 **Red Flags:**


- Multiple wire transfers just below reporting limits
- Transfers to high-risk offshore locations

 **Advanced Money Laundering & Terrorism Financing Techniques** **2.4.2 Using Special Types of Accounts** **2.4.2.1 Collection Accounts**

 **Used by foreign workers to remit money home**  

 **Illicit Use:** Criminal groups use these to **pool dirty money** before sending it abroad

 **Example:** A trafficker collects funds from multiple sources into **one account**, then sends a single international transfer.


 **Red Flags:**

- **Unrelated individuals making frequent small deposits into one account**
- **Large outgoing wire transfers to high-risk countries**

 **2.4.2.2 Payable-Through Accounts**

 **Foreign banks or companies open accounts at local banks**



 **Allows sub-account holders to conduct transactions anonymously**

📌 **Example:** A shell bank in Panama funnels funds through a US bank, allowing unknown foreign clients to move money.

🚨 **Red Flags:**

- Bank cannot verify account holders' identities
- High transaction volume from unknown sources

📌 2.4.3 Using Cross-Border Trade & Loans

🔍 2.4.3.1 Back-to-Back Loans

✅ Criminals transfer illicit funds abroad as “loan collateral”



✅ The loan is then sent back to the home country, appearing as legal income

📌 **Example:** A smuggler deposits ₹10 crore in Dubai as collateral for a loan, which is then legally transferred back to India.

🚨 **Red Flags:**


- Collateral-backed loans without legitimate business activity
- Large foreign deposits followed by immediate domestic loan disbursal

2.4.3.2 International Trade & Trade Finance

 **Over- or under-invoicing goods to shift illicit funds**

internationally  

 **Fake exports & overvalued imports used for money transfers**

 **Example:** A fraudster **pays ₹5 crore** for a **₹50 lakh shipment** of **fake goods** to shift money abroad.

 **Red Flags:**

- **Trade transactions inconsistent with market prices**
- **Frequent trade with high-risk jurisdictions**


2.4.4 Using Entities in Lax Jurisdictions

2.4.4.1 Offshore Banks

 **Banks in countries with weak AML laws accept illicit funds**



 **Common locations: Cayman Islands, Switzerland, Hong Kong**

 **Example:** A corrupt official moves bribes to a **Swiss bank account** under a **fake business name**.

 **Red Flags:**


- **Large remittances to offshore tax havens**
- **Sudden foreign bank transactions by an entity with no international presence**


JAIIB/ CAIIB/ PROMOTIONS/ CERTIFICATIONS Course available

<https://iibf.info/iibfLearning>

2.4.4.2 Shell Companies

 Fake companies with no real business operations  

 Used for fraudulent invoices, offshore banking & fake investments


 **Example:** A shell company in Dubai invoices ₹10 crore for fake consulting services, moving illicit funds offshore.

 **Red Flags:**




- Company registered offshore but has no physical operations
- Large transactions without a clear business purpose

 Advanced Money Laundering & Terrorism Financing Techniques




 2.4.5 Using Cards & Remittance Products

2.4.5.1 Credit & Debit Cards

 Criminals use structured payments to settle credit card bills in large amounts  

 Cash advances used to purchase demand drafts or wire transfers abroad

 **Example:** A fraudster **overpays a credit card bill using illicit funds**, then requests a refund to a clean account.

 **Red Flags:**

- Large credit card payments from multiple sources
- Frequent cash withdrawals from ATMs in different locations

 **2.4.5.2 Prepaid Cards**

✓ Criminals & terrorists use prepaid cards for anonymity 🎭 🏠

✓ Forex prepaid cards allow cash withdrawals globally without a bank account 🌐 💰

📌 **Example:** A terrorist group loads ₹50,000 onto multiple prepaid cards and withdraws the money near an international border.

 **Red Flags:**

- Multiple prepaid cards bought in cash by the same individual
- Large withdrawals from ATMs in different countries within a short time

 **2.4.5.3 Bureaux De Change (Money Changers)**

✓ Used to convert large cash amounts into foreign currencies




✓ Regulatory oversight is weaker compared to traditional banks



📌 **Example:** A trafficker exchanges ₹5 crore in small bills for larger foreign notes at an unregulated money changer.

 **Red Flags:**


- Frequent large currency exchanges by non-business customers
- Customers unwilling to provide ID or transaction details

 2.4.6 Using Other Remittance Services 2.4.6.1 Remittance Services

 **Criminals use informal remittance services to move illicit funds**

internationally  

 **Used to convert illegal cash into local currency in another country**

 **Example:** A fraudster in India sends ₹10 lakh via a remittance service, which is received as cash in Dubai.


 **Red Flags:**


- Frequent low-value international remittances from the same sender
- Transfers to high-risk jurisdictions without clear business purpose

2.4.6.2 Alternative Remittance Systems (ARS) / Value Transfer Systems

✓ These operate outside the formal banking system  

✓ Transactions occur between brokers using minimal documentation

 **Example:** A businessman deposits money with a **local broker**, who arranges for the same amount to be available at an overseas destination without moving actual currency.

 **Red Flags:**


- Transfers made with little or no documentation
- Settlement of funds through third parties instead of direct transfers

2.4.6.3 Hawala System

✓ Trust-based money transfer network with no formal records




✓ Common in South Asia & the Middle East for cross-border fund transfers

 **Example:** A terrorist financier in the UK gives ₹50 lakh to a **hawala broker**, who arranges for the same amount to be withdrawn in Pakistan without any electronic transfer.


 **Red Flags:**


- Large undocumented transactions in high-risk areas
- Transfers with no bank involvement or paper trail

 **Emerging Money Laundering & Terrorism Financing Threats** **2.4.7 Third-Party Products & New Technologies** **2.4.7.1 Insurance Policies**

 **Money launderers use insurance policies to clean illicit funds**



 **Common technique: Pay large premiums → Cancel policy → Get refund in another country**

 **Example: A fraudster pays ₹5 crore for a life insurance policy, cancels it in six months & requests a refund to an offshore bank.**

 **Red Flags:**

- Early policy cancellations with large refund requests
- Premium payments inconsistent with policyholder's income

2.4.7.2 Emerging Technologies & Internet Banking

 **Criminals use online banking, e-wallets & fintech platforms for laundering**  

 **No face-to-face verification makes tracking harder**

 **Example:** A hacker uses **crypto-based e-wallets** to send illicit funds globally within seconds.

Red Flags:


- **Multiple high-value transactions in a short time**
- **Funds transferred between different online wallets without justification**


2.4.8 Cybercrime & Cryptocurrency

2.4.8.1 Cybercrime & Online Fraud

 **Criminals use phishing, hacking & fraud to generate illicit funds**



 **Cybercrime allows rapid placement, layering & integration of funds**


 **Example:** A hacker steals **₹10 crore from an Indian bank** & wires it to offshore accounts in minutes.


Red Flags:


- **Unusual login activity & multiple high-speed transactions**

- **Massive fund transfers following cyberattacks**

2.4.8.2 Cryptocurrency & Virtual Assets

 **Cryptocurrency is widely used for money laundering & crime financing** ₿ 💰

 **Key risks: Anonymity, cross-border transactions, lack of regulation**

 **Example:** A fraudster launders **drug money via Bitcoin**, then converts it to real estate.

Red Flags:

- **Frequent high-value crypto transactions without clear sources**
- **Funds moving between multiple crypto wallets before liquidation**

Statistics:


- **Illegal crypto transactions hit \$14B in 2021, a 79% rise from 2020** 
- **Over 10,000 cryptocurrencies exist, making regulation difficult**




 **2.5 Sensitive Avenues for Money Laundering & Terrorism****Financing** **2.5.1 Gold & Diamond Markets** **2.5.1.1 Gold Market**

 **Gold is highly liquid, easy to smuggle & widely accepted**  

 **Launderers use fake invoices, smuggling & gold-backed loans**


 **Example:** A smuggler **buys ₹50 crore worth of gold bars**, sells them abroad & launders the money via shell companies.


 **Red Flags:**

- **Frequent high-value gold transactions without proper records**
- **Gold imports from high-risk countries without legitimate buyers**

 **2.5.1.2 Diamond Market**

 **Diamonds are used for terrorism financing & illicit trade**  

 **Small size, high value & anonymous transfers make them ideal for laundering**

 **Example:** A terrorist group **smuggles conflict diamonds**, sells them & funds attacks.

 **Red Flags:**

- **Frequent diamond transactions at unrealistic prices**

JAIIB/ CAIIB/ PROMOTIONS/ CERTIFICATIONS Course available

<https://iibf.info/iibfLearning>

- Trade involving known conflict zones

📌 2.5.2 Politically Exposed Persons (PEPs) & Corruption

✅ **Corrupt politicians & government officials launder illicit funds**



✅ **Use of shell companies, offshore accounts & luxury asset purchases**

📌 **Example:** A corrupt minister **moves ₹100 crore bribes via Swiss accounts & fake trusts.**

🚨 **Red Flags:**

- PEPs moving large funds with unclear sources
- Real estate purchases by individuals with political links

📌 2.5.3 Misuse of Non-Profit Organizations (NPOs) & Charities

✅ **Terrorist groups exploit charities for fundraising & money movement** 📄 🙌

✅ **Methods:**

- 1 Fake NPOs created to funnel funds
- 2 Legitimate charities infiltrated by criminals
- 3 NPOs used for money transfers disguised as humanitarian aid

📌 **Example:** A fake NGO collects **₹10 crore in donations**, but secretly funds militant activities.

🚩 **Red Flags:**

- **Charity receives large anonymous foreign donations**
- **Funds move from NPOs to high-risk conflict zones**

