🏦 REPORTING OBLIGATIONS OF BANKS

KYC/AML Chapter 10

🌐 10.1.1 PMLA/PMLR Stipulations

Under the **Prevention of Money Laundering Act (PMLA)** and the corresponding **Prevention of Money Laundering Rules (PMLR)**, banks are **required** to provide transaction information to the **Director, FIU-IND**. Specifically, **Section 12(1)(b) of PMLA** mandates:

"bb furnish to the Director within such time as may be prescribed, information relating to such transactions, whether attempted or executed, the nature and value of which may be prescribed;"

Rules **3** and **7** of **PMLR** (see **Annexure II**) specify the **reports** that must be submitted to FIU-IND.

10.1.1.1 Reports to be Submitted

Based on the aforementioned provisions, banks must submit the following **five** reports to FIU-IND, as shown in **Table 10.1**:

Sr. No	Report	Transactions to be Reported	Periodicity	Timeline
1	**Cash Transactions Report (CTR)**	1. All **cash transactions** exceeding **₹10 lakh** (or equivalent in foreign currency) 2. All **series of integrally connected** cash transactions (each below ₹10 lakh) within a month, where the aggregate exceeds ₹10 lakh	**Monthly**	By **15th** of the **next month**
2	**Suspicious Transactions Report (STR)**	All **suspicious transactions**, whether **cash** or **non-cash**, covering the categories listed under **Rule 3(D)**	**As & when**	Within **7 days** of determining suspicion
3	**Counterfeit Currency Report (CCR)**	**All cash transactions** involving **counterfeit currency notes** or where **forgery** of a valuable security/document has occurred	**Monthly**	By **15th** of the **next month**
4	**Non-Profit Organisation Transaction Report (NTR)**	All transactions **exceeding ₹10 lakh** (or equivalent in foreign currency) involving **non-profit organisations**	**Monthly**	By **15th** of the **next month**

Sr. No	Report	Transactions to be Reported	Periodicity	Timeline
5	**Cross Border Wire Transfer Report (CBTR)**	All **cross-border wire transfers** exceeding **₹5 lakh** (or equivalent) where the **origin** or **destination** of the fund is in **India**	**Monthly**	By **15th** of the **next month**

10.1.1.2 Delays/Non or Improper Submission

Rule 8(4) of **PMLR** specifies that each **day's delay** in submitting a required report **constitutes a separate violation**. Consequently, **non-submission**, **delayed submission**, or **incomplete reports** may trigger **penal actions** by the **Director, FIU-IND**, including **monetary penalties**.

10.1.1.3 Proper Internal Mechanism

Rule 7(3) of **PMLR** requires every reporting entity to maintain a **suitable internal mechanism** to detect and report the transactions listed above, following **regulatory guidelines**. A bank lacking **proper systems**, **procedures**, or **sufficient organizational setup** may face **penal actions** by the **Director, FIU-IND**.

🏦 10.1.2 RBI Guidelines

The **Reserve Bank of India (RBI)** has issued guidelines to help banks compile the **PMLA-mandated reports**. These guidelines can be found in **Master Directions – Know Your Customer (KYC) norms**, dated **February 25, 2016** (updated **May 10, 2021**).

- 📄 **Reporting Formats & Utilities**: RBI advises banks to refer to the reporting formats prescribed by FIU-IND, as well as the **Report Generation Utility (RGU)** and **Report Validation Utility (RVU)**.
- 💻 **Electronic Filing**: Banks yet to install automation tools for CTR/STR can use FIU-IND’s **editable electronic utilities** to compile and submit their **live transaction data**.
- 🏢 **Non-Computerized Branches**: If any branches are not **fully computerized**, the **Principal Officer** must arrange to obtain and **electronically consolidate** transaction details into **CTR/STR** files via FIU-IND’s electronic tools.

10.1.2.1 Suspicious Transactions Report (STRs)

- **Robust Software**: Banks should use **robust systems** that issue **alerts** when transactions appear **inconsistent** with the **customer’s risk profile** or **updated customer data**.
- **Reasonable Suspicion**: An STR should be filed if a bank **reasonably believes** a transaction **involves proceeds of crime**, **regardless of the amount**.

- **Abandoned/Aborted Transactions**: These must be **reported** as STRs **irrespective of their value**.
- 📝 **Reason Documentation**: The **Principal Officer** must **record in writing** the rationale for deeming a transaction suspicious.
- ⏰ **Timely Determination**: Avoid **unnecessary delay** in concluding whether a transaction is suspicious upon receiving a report from a branch or other unit.
- 📌 **Alert Indicators**: Banks should use parameters from **Annexures IX(1), (2)** & **XIII** (per **IBA's Guidance Note for Banks, July 2020**) for **risk-based transaction monitoring**.
- 🔎 **No Operational Restrictions**: Filing an STR **does not** justify imposing **transaction restrictions** on a customer's account.
- 🔒 **Confidentiality**: **No "tipping off"** the customer; STR filing details should be kept **strictly confidential**.

10.1.2.2 Counterfeit Currency Report (CCRs)

Apart from reporting **cash transactions** where **counterfeit notes** are detected, any transaction involving **forgery of valuable securities** or **documents** must also be reported to FIU-IND—these can be submitted in **plain text form**.

10.1.2.3 Non-Profit Organisation Transaction Report (NTR)

For the purposes of **NTR**, an **NPO** is any entity:

1. **Registered** as a **trust** or **society** under the **Societies Registration Act, 1860** (or similar State law), **OR**
2. **Registered** as a **company** under **Section 8** of the **Companies Act, 2013** (earlier **Section 25** of the **Companies Act, 1956**).

10.1.2.4 Cross Border Wire Transfer Report (CBWTRs)

A **CBWTR** must be filed for **all** cross-border wire transfers **exceeding ₹5 lakh** (or **equivalent** in foreign currency), where **either** the **origin or destination** of the funds is **India**.

📝 SUMMARY TABLE

Section	Focus	Key Points
10.1.1 PMLA/PMLR Stipulations	Legal requirement to submit reports to **FIU-IND**	• **Section 12(1)(b) of PMLA** • **Rules 3 & 7** of PMLR detail reporting obligations
10.1.1.1 Reports to be Submitted	Five primary reports (CTR, STR, CCR, NTR, CBTR)	Includes timelines (monthly or immediate) and details for reporting **cash**, **suspicious**, **cross-border**, **counterfeit**, and **NPO** transactions
10.1.1.2 Delays/Non-Submission	Penalties for missing or late reports	**Rule 8(4) of PMLR** treats each day's delay as a separate violation; can result in **monetary fines**

Section	Focus	Key Points
10.1.1.3 Internal Mechanism	Adequate systems & processes for transaction detection & reporting	Lacking such mechanisms can lead to **penal actions** by the Director, FIU-IND
10.1.2 RBI Guidelines	RBI's advice on compliance tools and software	Direct banks to use **FIU-IND utilities**, ensure complete coverage of **non-computerized** branches, etc.
10.1.2.1 STRs	Suspicious Transaction Reports	• **Robust alert software** • **No threshold limit** for STR • **Abandoned** transactions also included • **Confidentiality** to be maintained
10.1.2.2 CCRs	Counterfeit Currency Reports	**Cash transactions with counterfeit notes** or **forged documents** must be reported to FIU-IND
10.1.2.3 NTRs	Non-Profit Organisation Transaction Reports	Applies to **registered trusts, societies**, or **Section 8** (formerly **Section 25**) **companies**
10.1.2.4 CBWTRs	Cross Border Wire Transfer Reports	Must be filed for **all cross-border transfers** above ₹5 lakh if **either origin or destination** is in India

Below is a **rewritten** version of **Sections 10.2.1 through 10.2.2.3**, enriched with **emojis/icons** for better readability. **All original meaning and details are preserved**, and **no new content** has been introduced. A **summary table** follows at the end.

🏦 10.2 SALIENT ASPECTS OF REPORTING

🌐 10.2.1 Nature of FIU Reports

To fulfill their **reporting obligations** under the **PMLA**, banks must **monitor transactions** to identify which ones need to be reported.

10.2.1.1 Rule-Based – Threshold Value

Out of the **five** PMLA-stipulated reports:

1. **CTR (Cash Transactions Report)**
2. **NTR (Non-Profit Organisations Transaction Report)**
3. **CBTR (Cross Border Wire Transfer Report)**

…**four** are **rule-based** with **threshold limits**:

- **CTR**, **NTR**, and **CBTR** focus on **specific transaction types** exceeding a **particular value**.
- These can typically be generated **systematically** (e.g., via **Core Banking Systems**).
- If **CBS** is unavailable, relevant transactions must be collated at the **branch level** and then consolidated at the **Head Office**.

10.2.1.2 Rule-Based – Event of Counterfeit Notes/Forged Security

CCR (Counterfeit Currency Report) revolves around:

- **Detection** of counterfeit currency
- **Use** of forged documents/valuable securities in **cash transactions**

Banks need a system to forward **all such instances** to the **Head Office**, which then **compiles** the **CCR** for submission to **FIU-IND**.

Note: **CCR** to FIU is **distinct** from any reports the bank may submit to the **RBI** on counterfeit notes.

10.2.1.3 Norm-Based – Judgment of Genuineness

The **STR (Suspicious Transactions Report)** is **not** purely rule-based; it requires a **judgment call** on:

- **Legitimacy** (or lack thereof) of a transaction
- **Likelihood** that a transaction may serve an **illicit** purpose

Quantitative and **qualitative** data must be **reviewed** to decide if the transaction might not be **bonafide**.

10.2.1.4 Distinct Utility of Various Reports

- **CTR, NTR, and CBTR** provide **FIU-IND** with **massive** data on key transaction categories (cash, non-profit, cross-border). Much of that data is, however, **legitimate** business.
- **STR** has **particular importance** because it flags **unusual** or **suspect** transactions—essential leads that might be passed to **Law Enforcement Agencies (LEAs)**.

Key Point: While the bulk data (CTR/NTR/CBTR) is used to **supplement** suspicious leads, the **STR** is the primary driver for identifying **potential money laundering/terror financing** activities. Hence, **timely** and **accurate** filing of **STR** is **critical**, requiring:

- **Extensive monitoring**
- **Detailed customer due diligence**
- **Informed judgments** by bank officials

💰 10.2.2 Cash Transaction Reports (CTR)

When submitting **CTR**, consider the following crucial aspects:

10.2.2.1 Integrally Connected Transactions

CTR covers:

1. **Individual transactions** over **₹10 lakh**, **plus**
2. **“Integrally connected”** cash transactions within a **calendar month** that collectively exceed **₹10 lakh**.

Integrally connected transactions share these traits:

- They **all involve cash**.
- They are of the **same type** (**all deposits** or **all withdrawals**).
- They occur in the **same calendar month**.
- **Combined value** exceeds **₹10 lakh**.

  If **any single** transaction exceeds **₹10 lakh**, other smaller cash transactions in that month are also included in the **CTR**.
- They belong to the **same customer** acting in the **same capacity**.

  For example:
  - Deposits by Mr. X in **his personal savings account** plus deposits to **M/s. XX** (a **proprietary firm**), if it's owned **solely** by him, are **combined**.
  - But deposits made to **M/s. XYZ** (a **partnership** in which he's just one partner) might **not** be combined with his personal deposits.
- **Different purposes** by the same customer are still counted together.

  Example: Mr. X deposits **₹7 lakh in cash** to his **savings account** and also buys a **₹4 lakh Demand Draft** in cash. Both must be **grouped** for CTR evaluation.

Note: Individual transactions **under ₹50,000** need **not** be **reported** individually, but **do** count toward the **aggregate** total.

10.2.2.2 Transactions between Internal Accounts

Only **customer** transactions are reportable. **Inter-account transactions** within the bank (e.g., internal book entries) **are not** included in CTR.

10.2.2.3 Branch-Wise Reports

When **CTR** is **centrally generated** (e.g., in **Core Banking** setup):

- Prepare it **branch-wise**.
- A **copy** of each branch's CTR must be **available** at that branch for **auditors/inspectors**.

In branches **not under CBS**, the **branch** compiles and **forwards** its CTR to the **Principal Officer**, who then arranges the **final submission** to **FIU-IND** with a **bank-wide summary**.

📝 SUMMARY TABLE

Section	Key Focus	Essential Points
10.2.1 Nature of FIU Reports	Explains the **5 reports** under PMLA and why they're important	**4 are rule-based** (CTR, NTR, CBTR, CCR) with specific thresholds/events; 1 is **norm-based** (STR) requiring bank judgment on transaction genuineness.
10.2.1.1 – 10.2.1.2	**Rule-Based Reports** (Threshold/Event)	CTR, NTR, CBTR all use **value thresholds**; CCR triggered by **counterfeits/forged docs**. These

Section	Key Focus	Essential Points
		can be generated by **system** or manual if CBS is lacking.
10.2.1.3 – 10.2.1.4	**Norm-Based STR & Utility**	**STR** relies on **bank's assessment** of unusual transactions. STR is vital for identifying leads for **LEAs**. Other reports supplement STR's intelligence.
10.2.2 CTR	**Cash Transaction Reporting**	Must include **individual** > ₹10 lakh, plus **integrally connected** amounts if monthly sum > ₹10 lakh. Certain **exclusions** (internal bank accounts). Prepared **branch-wise**.

All details, structure, and meaning from the original text remain unchanged. Emojis/icons have been added for clarity and engagement.

Below is a **rewritten** version of **Sections 10.2.3 and 10.2.4**, enhanced with **emojis/icons** for clearer readability. All **original details, structure, and meaning** remain intact, and **no additional content** has been introduced. A **summary table** appears at the end.

🌐 10.2.3 Other Rule-Based Reports

10.2.3.1 Non-Profit Organisations Transactions Report (NTR)

Under **NTR**, banks must report **all individual receipts** above **₹10 lakh** in **Non-Profit Organisations (NPO)** accounts.

Definition: For **NTR** purposes, an **NPO** is any entity:

1. **Registered** as a trust or society under the **Societies Registration Act, 1860** (or similar State law), **OR**
2. **Registered** as a **company** under **Section 8** of the **Companies Act, 2013** (formerly **Section 25** of the **Companies Act, 1956**).

Therefore, such **NPO accounts** need to be **identified** and **categorized** accordingly.

🔍 *FCRA Requirements*

NPOs may also fall under the **Foreign Contribution Regulation Act (FCRA)**.

- Some **trusts** require specific **Ministry of Home Affairs (MHA)** approval to **receive foreign donations**.
- Any **foreign contributions** must be deposited only in **the account** specified in the **MHA permission letter**, and the **amount** is capped by the limits stated therein.

10.2.3.2 Cross Border Wire Transfers Report (CBTR)

CBTR covers **all cross-border transfers** exceeding **₹5 lakh** (or equivalent in foreign currency). This includes:

- **Inward** and **outward** foreign remittances

- **Any purpose** of transfer (e.g., imports/exports, investments, loans, miscellaneous remittances)

Some common **cross-border** transactions:

1. **Payments** for **imports/exports** of goods/services
2. **Investments** by residents in **non-resident entities**
3. **Loans** by residents to **non-residents**
4. **Investments** by non-residents in **resident entities**
5. **Loans** by non-residents to **residents**
6. **Miscellaneous receipts** from overseas to resident accounts
7. **Miscellaneous remittances** sent abroad by residents

10.2.3.3 Counterfeit Currency Report (CCR)

CCR applies to:

1. **Counterfeit currency** detected during the month
2. **Cash transactions** involving **forged documents** or **fake valuable securities**

1) Reporting Counterfeit Notes

- Must be reported **monthly** via **FINnet portal** (even a **single** counterfeit note).
- Accuracy is critical: banks also report **counterfeit notes** to **Police** and **RBI**, and **all these** records should match.

2) Fake Valuable Security / Forged Document

- Any **cash transaction** that uses a **fake security** or **forged document** must be reported to **FIU-IND**, **regardless** of transaction value.
- **No specific format** or **portal provision** for these cases; hence, banks typically send a **plain-text report** to the **Director, FIU-IND**.

🔎 10.2.4 Suspicious Transaction Reports (STRs)

STRs form the **cornerstone** of the **AML/CFT** framework. They provide **FIU** with **vital intelligence** to pass on to **Law Enforcement Agencies (LEAs)**. From a bank's perspective, **STR filing** usually requires the **most resources**, as it hinges on:

- **Customer due diligence**
- **Risk profiling**
- **Ongoing monitoring**
- **Identifying truly suspicious transactions**

Below are several key concepts:

10.2.4.1 Transaction – Definition

Per **Rule 2(h)** of the **PML Rules**, a **"transaction"** encompasses:

- Standard banking operations like **purchase**, **sale**, **loan**, **pledge**, **gift**, **transfer**, **delivery**, or their arrangements
- **Any activity** involving safe deposit lockers, fiduciary relationships, forming legal entities/arrangements, **payments made or received under any obligation**, etc.

Thus, typical banking (deposits, advances, remittances, trade products, etc.) and **non-fund services** (e.g., locker use, setting up new legal entities) are **all** considered "transactions" under PMLR.

10.2.4.2 Suspicious Transaction – Definition

Per **Rule 2(g)** of **PML Rules**:

1. **Covers all transaction types** under **PMLR** (see 10.2.4.1).
2. **Cash or non-cash** transactions, including **attempted transactions**, fall under scope.
3. **Any transaction** is deemed **"suspicious"** if, to a **reasonable person acting in good faith**, it appears to:
   - Involve **proceeds of crime** (covered by PMLA)
   - Have **unusual or unjustified complexity**
   - Lack **economic rationale** or a **legitimate purpose**
   - Possibly relate to **terrorist financing**

10.2.4.3 Suspicious Transaction Report – Distinctive Features

1. **Determining Criteria – Suspicion**
   - **Transaction value** is **irrelevant** (no threshold).
   - Both **fund-based** and **non-fund-based** activities can trigger suspicion.
   - The key factor is whether the **real purpose** looks **illegitimate** or **inconsistent** with the customer's known profile.
2. **Non-Fund-Based Services**
   - Applies equally to transactions like **locker usage** or **guarantees**.
   - Example: **Daily locker use** by someone with **no apparent reason** may be suspicious, whereas a **jeweler** frequently accessing a locker might be understandable.
3. **Transaction Value**
   - **Even low-value** transfers can matter, especially if linked to **terrorist financing**.
   - Sometimes, **numerous small** transactions might collectively indicate ML/TF risk.
4. **Non-Monetary Transactions**
   - Activities **without** direct **movement of funds** (e.g., creating multiple shell companies or trusts) can still be suspicious.

5. **Attempted Transactions**
   - **PML Rules** mandate reporting **attempted** or **aborted** dealings if they **raise suspicion** of money laundering or terrorist financing.
   - Even if the **customer** ultimately **does not** perform the transaction, an **STR** may still be necessary.
   - The **Cobrapost** episodes underscore that banks can face penalties for **not filing** STRs in suspicious "attempted transaction" scenarios.

📝 SUMMARY TABLE

Section	Focus	Key Points
10.2.3.1 NTR	Non-Profit Organisations Transactions Report	All **receipts** >₹10 lakh in **NPO** accounts. Includes **FCRA** considerations when receiving foreign funds.
10.2.3.2 CBTR	Cross Border Wire Transfers >₹5 lakh	Covers **inward/outward** remittances **exceeding** threshold. Includes **imports/exports**, **loans**, **investments**, etc.
10.2.3.3 CCR	Counterfeit Currency / Forged Documents	**Monthly** report for **counterfeit notes** (no threshold). **Any** cash transaction using **forged documents** also reported to FIU-IND in **plain text**.

Section	Focus	Key Points
10.2.4 STR	Suspicious Transaction Reports	**Cornerstone** of AML/CFT; no threshold. Covers both **actual** and **attempted** transactions – including **cash, non-cash**, and **non-fund-based**.
10.2.4.1 & 4.2	Definitions of "Transaction" & "Suspicious Transaction"	**PML Rules** define transactions broadly. A transaction is "suspicious" if it appears to involve **proceeds of crime**, is **unusually complex**, or lacks **legitimate purpose**.
10.2.4.3	Distinctive Features of STR	**Suspicion** is the key factor. **Value**, **mode**, or **completion** of the transaction is secondary. **Attempted** transactions also qualify for **STR**.

All details, structure, and meaning remain unchanged. Emojis/icons have been added for clarity and engagement.

Below is a **rewritten** version of **Sections 10.3.1 and 10.3.2**, enhanced with **extensive emojis/icons** to improve clarity and readability. **All original meaning, structure, and details remain unchanged**, and **no additional content** has been added. A **summary table** is included at the end.

🔍 10.3 TRANSACTION MONITORING

🌐 10.3.1 Objectives and Norms for Monitoring

Ongoing monitoring of customer transactions is critical for an effective **AML/CFT** regime. This monitoring serves two main objectives:

1. **Consistency Check**: Ensure that transactions align with the **customer's profile**.
2. **Regulatory Reporting**: Facilitate submission of prescribed **FIU-IND** reports.

Because it's **impractical** to monitor **all** transactions with the **same level** of diligence, banks employ a **Risk-Based Approach (RBA)**, as recommended by **FATF**. This means:

- **High-risk customers** (e.g., PEPs, complex corporates, multi-country businesses) are subject to **enhanced scrutiny**.
- **High-risk products/services** (e.g., import remittances, FDI, commodity/diamond trade) undergo closer transaction reviews.
- **Other scenarios** potentially calling for intensified checks include:
  - Unusually **large** or **complex** transactions
  - Transactions near/above **set thresholds**
  - **Cash** transactions inconsistent with a customer's usual activity

- **High turnover** or **very quick movement** of funds in an account, not matching its typical balance

⚙️ 10.3.2 Methods for Monitoring

Banks generally use a **combination** of techniques to monitor customer transactions. These methods fall into **three** broad categories:

10.3.2.1 Observation-Based

Bank staff, particularly at **branches** and **operating units**, may notice **unusual transactions** or suspicious **customer behavior**. A **mechanism** must exist for staff to **report** such observations to the **AML cell** for detailed analysis. This approach is often **vital** for identifying **attempted transactions** (ones **not** completed, yet suspicious).

Examples of Indicators (from **IBA Guidance**, Annexure XIII):

- A customer **refuses** to open an account upon learning about **KYC** norms.
- A customer **abandons** a transaction after being asked about the **source of funds**.
- A customer is consistently **accompanied by unrelated** individuals.
- The customer's **ID documents** appear **altered** or **forged**.
- Use of **complex legal structures** or **beneficial ownership** that's difficult to ascertain.

- **Media reports** link the customer to criminal offenses.
- **Foreign remittance** received by an NPO **not** approved under **FCRA**.
- Complaints of the account being **misused** for fraud.

First Line of Defense:

- The **business/operations** teams handle **sale** and **execution** of transactions, ensuring compliance with **regulations** and **risk checks**.
- Integrating an **ML/TF perspective** at this level significantly enhances **transaction monitoring** effectiveness.

10.3.2.2 Exception Report-Based

Another technique is to generate **exception reports** from:

- **Core Banking Systems (CBS)**
- **Other transaction-processing** applications

The **exception reports** highlight **deviations** from normal patterns. Bank officials then:

1. Compare the flagged transaction(s) against the **customer's known profile** and historical activity.
2. Conduct additional inquiries to confirm if the transaction is **legitimate** or could be **suspicious**.

10.3.2.3 AML Software-Based

Manual oversight alone is insufficient, given:

- **High volume** of transactions/customers
- **Diverse** product/service lines
- Automated **straight-through processing** (e.g., online transactions)

Hence, banks deploy **specialized AML software** capable of:

- Providing **comprehensive** coverage of all transactions
- Using **rules** to detect **various suspicious patterns**
- Linking multiple products/accounts **held by the same customer**

🔎 **RBI's KYC Directions** require banks to have **robust software** that triggers **alerts** for transactions **inconsistent** with a customer's **risk category** or **profile**.

The **specific choice** of AML software and its features depends on:

- **Bank's product** portfolio
- **Transaction volumes/values**
- **Customer base** size and complexity

📝 **SUMMARY TABLE**

Section	Focus	Key Points
10.3.1	**Objectives & Norms** for Transaction Monitoring	Ensures **profile consistency** and **reporting compliance**. Involves **Risk-Based Approach** (RBA): higher scrutiny for high-risk entities.
10.3.2.1	**Observation-Based** Monitoring	Branch staff observe **unusual behavior** or patterns. Crucial for identifying **attempted transactions** that never finalize.
10.3.2.2	**Exception Report-Based** Monitoring	**Core banking** and other systems generate **alerts**. Staff validate these exceptions with **customer profiles** and transaction history.
10.3.2.3	**AML Software** for Comprehensive Monitoring	Software checks large transaction volumes. **RBI** mandates **robust** solutions to flag inconsistencies with **risk categories**.

All details and the original structure remain unchanged. Emojis/icons have been added for clarity and engagement.

Below is a **rewritten** version of **Sections 10.3.3 and 10.3.4**, enhanced with **extensive emojis/icons**. **All original meaning, details, and structure** have been retained, and **no additional content** has been added. A **summary table** appears at the end.

⚙️🔍 10.3.3 Rules for Generation of Alerts

AML software efficacy depends heavily on **alert-generation rules**. Banks must strike a balance between **broad coverage** (catching a wide variety of suspicious patterns) and **manageable volumes** of alerts for **meaningful analysis**.

🏦 **RBI** has advised banks to adopt **IBA Working Group** scenarios (Annexures IX(2) & XIII), with a few exceptions. These scenarios typically involve:

- **Matching** customer details with various **watch lists** (e.g., UNSCR, UAPA-designated, Interpol, OFAC, etc.)
- **High-value** deposits/withdrawals in a single day/month
- **Sudden** large transactions not consistent with the customer's past pattern
- **New accounts** with unusually high activity
- **Splitting** of cash transactions below threshold values
- **Multiple** accounts routing funds (one-to-many / many-to-one)
- **Small repeated** withdrawals in sensitive locations
- **Large debit balances** on credit cards or big-value card purchases
- **Loan repayments** in cash
- **Early closure** of large deposits via demand drafts/pay orders
- **Frequent** operations of safe deposit lockers

- **Inward foreign remittance** inconsistent with customer's profile
- **High-value** transactions with tax havens
- And more…

🚢 10.3.3.1 Specific Rules for Trade-Based Money Laundering (TBML)

A significant portion of money laundering is **trade-based**. Banks handling **global transactions** should deploy specialized **TBML** checks, focusing on **unusual** or **inconsistent** trade behaviors. Examples include:

- **Inward remittance** quickly withdrawn/transferred
- Customer in a **high-risk** business sector
- **Brief** account lifecycle used only for **advance remittances**
- Amount of **advance** not aligned with typical **trade practice**
- Transactions involving **intangible goods** (e.g., e-codes, PINs, specialized software)
- High proportion of **high seas sales** or **merchanting trades**
- Using **exchange centers** for funds despite having **bank** accounts
- **Vague** goods descriptions
- **Suspicious** or incomplete trade documents
- Payments for **old** import bills with no proper justification
- **Missing** originator/beneficiary details in wire transfers
- **Repeated LC amendments** without sufficient rationale

- **Unclear** value/quantity of goods
- **Repetitive** export/import of the **same** high-value item
- **LC** with **unusual** or **non-standard** clauses

⚙️ **Key Point**: Effective monitoring of trade transactions requires **extensive data capture** (e.g., shipping documents, invoices, etc.) and thorough **scrutiny** of related documentation. Having **comprehensive systems** to gather trade-related info helps the **AML** application detect suspicious activity more accurately.

🔎 10.3.3.2 Analysis of Alerts

Not every **alert** from AML software indicates a genuine **suspicious** transaction. These alerts merely **flag** potential concerns (so-called "**false positives**" are common). Therefore:

1. **AML analysts** must review each alert in light of:
    - Customer **profile**
    - Historical transaction **patterns**
    - Any **associated** relationships or accounts
2. The review helps determine if the transaction is **legitimate** or **potentially suspicious**. Ready access to **customer information** (e.g., KYC, past transaction history) makes this process **more efficient** and **accurate**.

⚙️ 10.3.3.3 Fine-Tuning of Alerts Generation

To reduce **false positives**, banks can employ techniques such as:

1. **White Listing**
    - Accounts proven to be **genuine** can be **whitelisted** for certain rules, preventing **repetitive** alerts.
2. **Rules Management**
    - Different products/services may need **tailored** rules based on unique **characteristics**.
    - Customer **risk profiles** and **typologies** of suspicious transactions (STR patterns) inform the creation of **specialized** rules.
    - Rules can also vary by **geographical** or **sector-specific** factors, minimizing **irrelevant** alerts and reducing "**false negatives**."
3. **Threshold Setting**
    - The **number** of alerts is often tied to **threshold values** in each rule.
    - Determining optimal thresholds requires **statistical analysis** of historical data—comparing alerts triggered under varying thresholds.
    - Aim is to find a **sweet spot** minimizing both **false positives** and **false negatives**.

🤖 10.3.3.4 Advanced Technology for Transaction Monitoring

For **large** and **complex** banks, more **sophisticated** IT solutions (AI, ML, RPA) can:

- **Automate** early-stage alert reviews
- Use **data science** and **digital footprints** to detect anomalies
- **Consolidate** and analyze **historical** data to identify suspicious trends

Key capabilities might include:

- **Network analysis**
- **Fuzzy-matching algorithms** & intelligent **scoring**
- **Alert consolidation** (grouping multiple alerts by the same customer)
- **Peer-group & historical anomalies** detection
- **Secure** multi-server deployment
- **Auto-closure** of trivial alerts
- **Real-time** transaction monitoring & alert investigation
- **Unstructured data** linkage

🏦🔐 10.3.4 STR Propositions and Approval

Whenever a transaction is flagged as **potentially suspicious**—whether:

1. From a **branch/operational** referral,
2. An **exception report**,
3. Or an **AML software alert** (surviving the weeding-out process)—

…it undergoes a **detailed** check by **AML analysts**, who:

1. Study all relevant transaction **documents**
2. Request **additional** information from the customer if necessary
3. Form a **reasoned opinion** on whether to file an **STR** or **not**

The **Principal Officer** ultimately **approves** and **signs** off on the STR, documenting the **"Grounds of Suspicion."**

📥 10.3.4.1 Preparation and Filing of STRs

Filing an STR requires **complete and accurate** details:

- **All** relevant accounts, individuals, or entities tied to the suspicious scenario
- **Key identifiers** (PAN, ID number, Date of Birth, etc.)
- A **comprehensive** "Grounds of Suspicion" section detailing the **background** and **context** (including customer relationship history)

This data assists **FIU-IND** in determining:

- **Next steps** (whether to forward to **Law Enforcement Agencies**)
- **Usefulness** in any official investigation

Finally, the STR is **filed** through the **designated reporting portal** provided by **FIU-IND**.

📝 SUMMARY TABLE

Section	Focus	Key Points
10.3.3 Rules Generation	Crafting **broad yet targeted** AML alerts	Align **alert thresholds** & **filters** with business patterns. Rely on recommended **IBA scenarios** plus custom rules for **TBML** or high-risk activity.
10.3.3.1 TBML	**Special checks** for **Trade-Based** ML	Spot irregularities in **trade docs**, suspicious **amendments** to LCs, vague item descriptions, high-value repeated exports/imports, etc.
10.3.3.2 Alert Analysis	Differentiating **false positives** from real suspicion	Analysts compare alerts with a customer's **profile** & **history**; legitimate transactions are cleared, suspicious ones escalated.
10.3.3.3 Fine-Tuning	Reducing false positives/negatives	Techniques: **White Listing**, **Rules Management**, **Threshold** adjustments. Statistical analysis of alerts helps refine system accuracy.

Section	Focus	Key Points
10.3.3.4 Advanced Tech	**AI/ML/RPA** for more powerful monitoring	Enables **real-time** checks, **network** analysis, and advanced **fuzzy matching**. Facilitates **faster** & **smarter** triage of alerts.
10.3.4 STR Approval	Escalating potential suspicions to the **Principal Officer**	Thorough evaluation of flagged transactions. Final **STR** includes all **relevant details** and comprehensive **Grounds of Suspicion**.

Below is a **rewritten** version of **Section 10.4.1 (Cases with Inland Transactions)**, presented with **extensive emojis/icons**. **No new information** has been added, and **all original meaning, details, and structure** remain intact. A **summary table** appears at the end.

💡 10.4 STR TYPOLOGIES 💡

Money launderers use **various methods** to mask the origin of illicit funds. Below are some **typologies** observed in suspected money laundering (ML) cases **within** national borders (**inland transactions**).

🏛️ 10.4.1 Cases with Inland Transactions

🔹 (i) Common Remitters / Shell Entities

- **Scenario**
  - **M/s. XYZ Ltd.** (Directors: **Mr. A** and **Mr. B**) opened a current account, declaring the business as "Trader."
  - After ~18 months of near **zero activity**, the account suddenly received **large** internal transfers from **eight private limited companies** and **RTGS** credits from **two companies** over 10 months.
  - Funds were **immediately** sent (via **RTGS**) to **four firms**, and part was looped back to **three** of the original eight accounts.
  - A similar pattern occurred in the current account of **M/s. POR Ltd.** (Directors: **Mr. C** and **Mr. D**), opened around the same time and at the **same branch** with a declared "Trading" activity.
  - Field inquiries revealed **both companies** did **not** exist at the provided addresses.
- **Indicators**

0. **Sudden surge** in account activity after a dormant period.
1. **Inward RTGS** immediately **re-routed** to other entity accounts in the same/other banks.
2. **Same remitters** sending funds into **both** accounts.
3. Companies **not found** at their given address → **Shell entities**.

- **(ii) Multiple Level Marketing (MLM) Related Activity**
  - **Scenario**
    - **Mr. A** opens a **savings account**, stating he is **salaried**.
    - Within **3 months**, numerous **small-value cash deposits** flow in, summing to **1.5×** his stated annual income.
    - Immediately after deposits, he withdraws the amount via **multiple DDs** favoring **M/s. XYZ Ltd.**
    - Investigations show **M/s. XYZ Ltd.** is involved in **MLM** (multi-level marketing), receiving cash from garment buyers. The internet also showed **numerous complaints** against the company.
  - **Indicators**

    0. Large **volume** of **small cash deposits** in an individual's **savings account**.
    1. **Multiple demand drafts** issued in the **same name** on the **same day**.
    2. **Mismatch** between transaction pattern and a "salaried" profile.
    3. **MLM** involvement uncovered upon inquiry.
    4. **Public complaints** against the MLM company.

- **(iii) Multiple Shell Entities**

- **Scenario**
  - **M/s. XYZ Ltd.** (Directors: **Mr. A**, **Mr. B**) opened a current account (trading in cloth). They are also directors of **3 other companies** (**M/s. ABC Ltd.**, **M/s. DEF Ltd.**, **M/s. PQR Ltd.**) at the **same branch**.
  - **M/s. LMN Ltd.** (Directors: **Mr. C**, **Mr. D**) also opened an account for "Trader" activity at the same branch. **Mr. C** and **Mr. D** were also directors in **3 other companies** at the same branch.
  - **All companies** shared the **same address**, **same email ID**.
  - In 5 weeks, **M/s. XYZ Ltd.** surpassed **60%** of its declared **annual turnover** in credits.
  - Cash deposits <₹10 lakh from **7** accounts → funnelled into **M/s. XYZ Ltd.** account → part of it moved via NEFT to **another bank** → from there, **RTGS** to 3 different companies.
  - None of the companies **existed** at the given address; directors couldn't be found, and their provided **driving licences** were **fake**.
- **Indicators**
  0. **Sub-threshold** cash deposits across multiple accounts (under **₹10 lakh**) aggregated into one.
  1. **Immediate** outflow of funds once consolidated.

2. **No** genuine business transactions.
3. **Shared** address/email for multiple entities.
4. **Fake** ID proofs.
5. Entities were **shell companies**.

(iv) Benami Entity / MLM Activity

- **Scenario**
  - **M/s. ABC** (Proprietor: **Mr. A**) declared "Trading" as the activity. In 18 months, credits exceeded **6×** the declared annual turnover.
  - **Over 5700** small cheques (round figures like ₹1250, ₹2000, ₹2250) were deposited, 20% of which **bounced**.
  - **80%** of the funds withdrawn **in cash**, the remainder via NEFT/cheques.
  - No **trace** of the firm at its stated address. **Mr. A** turned out to be employed as a **manager** at another company with a **similar** name.
- **Indicators**

0. **Huge** volume of small, round-figure cheque deposits.
1. **High bounce rate** (20%).
2. **Immediate** cash withdrawals.
3. **No** real business activities shown.
4. The actual "firm" does **not exist** at the given location.

5. Mr. A's **employment status** conflicts with "proprietor" claims → **benami** structure.
6. **Fixed** denominations, many small cheques → indicative of **MLM** pattern.

🔹 **(v) Shell Entities / Sudden Spurt**

- **Scenario**
  - At a **jewelry-market** branch, **M/s. ABC** (Proprietor: **Mr. A**) opened a current account for **import/export**. Two **similar** proprietorship firms started around the same time, including **M/s. XYZ**.
  - After ~30 months of **negligible** activity, both **M/s. ABC** and **M/s. XYZ** had a **rapid increase** in transactions over 12 months.
  - In **M/s. ABC**, credits primarily came from **9 entities** (via RTGS/NEFT), **2 entities** (internal transfers), and occasional cheque deposits. Funds were quickly paid out to **7** other entities or withdrawn in **cash (15%)**.
  - **M/s. XYZ** followed the **same** pattern. Both firms had the **same address**, which turned out **non-existent**. The **same mobile number** was given for multiple entities, owned by **Mr. B**, a proprietor of another entity in the **fund flow chain**.

- **Indicators**
    0. **Sudden** upswing in account activity.
    1. **High-risk** trade sector (jewelry market).
    2. **No** genuine commercial deals.
    3. Accounts **operated** by someone other than the official proprietor (benami structure).
    4. **Shared address** and **common mobile** for many entities.
    5. Firms **not** located at the stated address.
    6. Mobile number **belongs** to a **third party**.

(vi) No Economic Rationale

- **Scenario**
    - **M/s. ABC** & **M/s. DEF** (Proprietor: **Mr. A**, both "Stock broking") opened current accounts within a month.
    - In ~18 months, **M/s. ABC** reached **6.5×** its declared annual turnover, with credits from cheques, internal transfers, and some cash. Debits went to **various individuals** via multiple cheques and internal transfers. **M/s. DEF** had a similar but smaller-scale pattern.
    - Neither entity existed at the stated address, and the proprietor was unreachable at the given mobile number.
- **Indicators**
    0. Numerous cheque deposits, quickly paid out to multiple **individuals**.

1. Claimed "stock broking," but **no** actual stock-related activity.
2. Firms do **not** exist at stated location.
3. The proprietor's **contact** info is invalid.

📝 SUMMARY TABLE

Typology / Case	**Main Red Flags**	**Key Observations**
(i) **Common Remitters** / Shell Entities	**Dormant** → **Sudden high activity**, same **remitters** to multiple accounts, shell co. not at address	**Immediate** RTGS outflows, funds cycled among multiple accounts, shared or invalid addresses
(ii) **MLM**-related	Numerous **small cash deposits**; multiple DDs to same entity	Pattern **incompatible** with a "salaried" profile. Entity has **negative** public reputation (MLM).
(iii) **Multiple Shell Entities**	Complex network of **multiple companies** with same directors/addresses	**Fake** IDs, sub-threshold transactions that converge into a single account, no real **business**.
(iv) **Benami / MLM**	Large numbers of **small cheque** deposits, many **bounced**	**Fake** or **non-existent** business premises, proprietor also employed, possibility of **MLM** scheme.

Typology / Case	Main Red Flags	Key Observations
(v) **Shell Entities** / Spurt	**Negligible** activity, then **sudden** large-volume transactions	**Common** address/phone for multiple "firms," 15% **cash** withdrawal, high-risk sector (jewelry).
(vi) **No Economic Rationale**	Claimed "stock broker" but no actual stock transactions, addresses invalid	**Large** turnover vs. declared figure, inconsistent with **stated** business, non-contactable proprietor.

Below is a **rewritten** version of **Sections 10.4.2, 10.4.3, 10.5, 10.5.1, 10.5.2, 10.5.3, and 10.5.4**, featuring **extensive emojis/icons** for visual clarity and emphasis. **All original meanings, details, and structure** are preserved, with **no additional** content introduced. A **summary table** appears at the end.

🌐🔍 10.4.2 Cases with Cross-Border Trade Transactions

(Trade Based – Multiple Shell Entities)

🏦 (i) Cross-Border Remittances / Shell Firms

- **Scenario**
    - **M/s. XYZ** (Proprietor: **Mr. A**) declares **Import/Export** (steel coils) as its activity upon opening a current account.

- Within **6 months**, the account receives **large inward RTGS** credits from **seven** proprietorship/partnership firms.
- Funds are then **instantly remitted overseas** to **four** entities.
- **On-site verification** reveals the firm **does not exist** at the stated address; the proprietor is **unreachable** by the mobile number given.
- A "de-duplication" process shows **five** more current accounts under **Mr. A** (various identities: proprietor/director). One was **M/s. PQR** (Proprietor: **Mr. B**), but the photo used matches **Mr. A**. Four accounts were private limited companies where **Mr. C** was a director, again the **same photo** as Mr. A.
- **Six** other current accounts are also linked by receiving RTGS from the **same** set of remitters.

- **Indicators**

0. **High-value** credits into a newly opened account.
1. **Immediate** overseas remittances.
2. **Same remitters** appear in **multiple** accounts with **fake** identities.
3. Some **remitter firms** also receiving RTGS from others in this group.
4. Firm not found at the **registered address**.

5. Proprietor **not contactable**.

(ii) Trade Remittances / Unrelated Activities

- **Scenario**
  - **M/s. ABC Ltd.** (Directors: **Mr. A, Mr. B**) claims **Import/Export** of "Machinery, Tools, Hardware."
  - Over ~1 year, credits in the account are **<5%** of the declared turnover, mostly **RTGS/NEFT** from various entities.
  - Funds are either **sent overseas** or **(10% of them)** RTGS/NEFT to domestic entities.
  - **Company** is non-existent at its stated address.
  - Two **other** accounts at the same branch receive **similar** RTGS credits from the **same** remitters, with the same immediate **outward** forex transfers.
  - Both the private limited company and a partnership firm are found to have **mismatched** lines of business. Upon requesting supporting documents, **they close** their accounts.
- **Indicators**

0. **Common** set of remitters for entities in **different** businesses.
1. Actual turnover is **far** below stated annual figures.
2. **Declared** line of activity differs from **real** operations.
3. Company **not located** at stated address.
4. **Immediate** outward forex transfers after receiving funds.
5. **Closure** of accounts when asked for documentation.

🏦 (iii) Trade-Based / Account Closed in Short Span

- **Scenario**
  - **M/s. ABC** (Proprietor: **Mr. A**) declares **Import** of "electronic goods, cereals."
  - Within **3 months**, turnover is ~**40×** the stated annual turnover.
  - In **2 months**, **61** outward forex remittances (over **15×** the declared turnover) go to **one** entity in **Hong Kong**.
  - All outward remittances are **below USD 100,000**—thus **no Bill of Entry** required.
  - The account is mainly funded by **cheques/transfers** (~65%) and **cash** (~35%). Unused funds (besides outward remittances) are **withdrawn in cash**.
  - After 3 months, the account **goes dormant**.
- **Indicators**

0. **Mismatch** in declared imports vs. actual commodities.
1. Extremely **high turnover** in a very **short timeframe**.
2. All payments to **a single overseas beneficiary**.
3. **High-risk** import item + **high-risk** destination country.
4. Remittance **below** USD 100k each → no mandatory docs.
5. Account **inactive** after a brief flurry of transactions.
6. **No** other business activity.

🖥️⚠️ 10.4.3 Cases Related to Cybercrime & Crypto Currencies

🔹 (i) Ransomware Attack on Computer Systems

- **Example: Wannacry** Ransomware Attack (2017)
  - Thousands of **computer systems** globally were infected, including hospitals and banks.
  - Victims paid **ransom** in **Bitcoins** to a **public** Bitcoin wallet.
  - The hackers **moved** these Bitcoins through multiple transactions into various asset forms, then tried converting them to **fiat** (traditional) currency.
  - Authorities **blocked** the funds (~USD **100 million**) before the hackers could retrieve them. Damages to affected institutions topped ~USD **8 billion**.

(Source: Virtual Assets: What, When, How? – Hand Guide, FATF)

- **(ii) Cryptocurrency (OneCoin) Euro Fraud**
  - **Scenario**
    - A company in **Country A** (Southeast Europe) has **four** shareholders (two local, two foreign from **Country B**).
    - It sells **online tutorial** packages for investing in "**OneCoin**."
    - One foreign shareholder has a **criminal record** and **unpaid taxes** in his home country.
    - Data analysis uncovers ties between **OneCoin** and another firm in **Country C** (Central America), where local authorities had **banned** business with that firm.
    - Funds from the **Country A** account were sent abroad under the guise of **payments** to jewelers in **Country B**.
    - **OneCoin** was marketed as a crypto, raising **billions of euros** globally via educational packages.

(Source: Best of Egmont Cases 2014–2020, Egmont)

- **(iii) Cyberattack Through SWIFT Heist**
  - **Scenario**
    - In **October 2017**, a large **Asian** commercial bank in **Country A** fell victim to a **multi-layered cyberattack**.
    - Hackers **compromised** user accounts and issued **31 fraudulent SWIFT transfers** to **21 banks** in **9 countries**.
    - Attack timing exploited a **long holiday closure**.

  - The bank's **Trade** and **Compliance** teams reacted quickly, blocking most funds at receiving banks.
  - Prompt reporting to **FIU** and multi-country coordination resulted in freezing the rest of the stolen funds.

(Source: Best of Egmont Cases 2014–2020, Egmont)

🏦🔎 10.5 AML Monitoring and Fraud Prevention

Frauds pose a significant threat to banks, and **transaction monitoring** can help detect not only **money laundering** but also **fraudulent** activities. Some **alert** scenarios (e.g., large transactions in new accounts, mismatch of declared income, etc.) may reveal both **ML** and **fraud**.

Often, banks use a **common software and team** for **AML** and **Fraud** prevention to handle system-generated alerts jointly. Specific **fraud-detection rules** can complement AML checks, providing integrated oversight.

🕵️💰 10.5.1 Customer-Induced Frauds

- **Typical Indicators**
  - **Short** account lifespan
  - Rapid **withdrawal** of the initial funding

- High-value transactions from **other branches/cities**
- **ATM** or **POS** usage with large limits
- Sudden **inflow** of RTGS followed by quick **cash** or **ATM** withdrawals
- **Rented** address premises

📝 (i) Fraudulent RTGS – Walk-In Customer Account

- **Scenario**
  - A **savings account** opened by a "walk-in" customer.
  - Initial **small** funding, declared occupation as **trader**, but 2 months of **no** real activity.
  - Suddenly, a **₹5 lakh RTGS** credit arrives.
  - Over the next week, funds are withdrawn via **cheque** at the counter, **ATMs** in other cities, or **POS** payments.
  - The balance left is <₹500. Later found that the **₹5 lakh** RTGS was **fraudulently** sent from another bank account.
- **Indicators**

  0. **Dormant** account for ~2 months.
  1. **Nominal** deposits not matching "trader" profile.
  2. Sudden **high-value RTGS** in a new, inactive account.
  3. Quick **cash**/ATM withdrawals in distant locations.

📝 (ii) Fraudulent RTGS – Current Account of Proprietorship

- **Scenario**
  - Opened with **KYC** of proprietor, plus two firm documents; declared activity as **Trader**.
  - Field verification: operating from **residence**.
  - For ~1 year, multiple **RTGS credits** from a single remitter, withdrawn **in cash**.
  - Alerts triggered for **high-value credits** but closed as "commission payments."
  - Eventually, a **₹5 lakh RTGS** arrives, largely **withdrawn in cash**.
  - After 2 weeks, the remitting bank discloses the transfer was **fraudulent**.
  - The voter ID of the customer was **not** found in official records.
- **Indicators**
  0. No **real** commercial premises for a "trader."
  1. All **cash** withdrawals, unusual for a business.
  2. Transaction pattern doesn't match declared occupation.
  3. Documents not **verified** in official databases.

📝 (iii) Current Account of Proprietorship Firm

- **Scenario**

- Declared line of business: **Garment trader**; initial funding from proprietor's savings account.
- Multiple **NEFT credits** labeled as "duty drawback," but **no** apparent **trading** activity.
- Submitted **export** documents mention goods like **cotton/polyester**, not matching "garment" business.
- **Customs** instructs bank to **block** the account.

📝 (iv) Money Mules

Criminals use "**money mules**" to move fraudulent or illicit proceeds, often in exchange for a **commission**. Mule recruitment may happen via **spam emails** or **fake job ads**. Indicators:

1. **Third parties** always handle the account; actual owner is absent.
2. **Account holder** is unreachable or **unwilling** to discuss transactions.
3. Transactions **inconsistent** with declared business or profile.
4. Complaints from depositors who responded to suspicious **job/lottery** ads.

Tip: Following **KYC** protocols and **transaction monitoring** helps banks spot **money mules**. If an account is suspected, file an **STR**.

🏦🔐 10.5.2 Staff-Related Frauds

Despite internal **checks** and **controls**, **insider** fraud can occur. Some **warning signs** of potential staff involvement:

- **Lavish** or **unexplained** lifestyle
- **Avoidance** of taking **long leave**
- Repeated **rule-breaking** or **negligence**
- Making **frequent deposits** on behalf of others

Mitigation tactics include **job rotations** and **mandatory annual leave** to reduce the window for fraudulent activity.

💼🔏 10.5.3 Staff Callousness

Sometimes **employees** may **inadvertently** aid fraudsters by **disclosing** internal **bank policies** or procedures. Staff should be **trained** not to share **confidential** info that can help fraudsters exploit system weaknesses.

📝🔎 10.5.4 Common Precautions on New Accounts

Over time, banks have implemented certain **standard safeguards** for newly opened accounts:

- **"New Account"** notation on cheques
- **System alerts** for new accounts
- **High-level approvals** for large payments
- **Enhanced scrutiny** for substantial transactions

- Carefully **examining** instruments dated **prior** to the account opening
- **Verifying** with the **drawer/drawee** bank if needed

📝 SUMMARY TABLE

Section	Focus	Key Points
10.4.2 (i)-(iii)	**Cross-Border Trade / Shell Entities**	Large **RTGS in** → **Immediate** overseas transfers, shell companies, short account lifespans, mismatch of declared vs. actual business.
10.4.3 (i)-(iii)	**Cybercrime & Crypto**	**Ransomware** (Wannacry), **OneCoin** crypto fraud, **SWIFT** heists. Use of advanced technology & cross-border coordination key to blocking funds.
10.5 AML Monitoring	**Fraud Prevention Synergy**	Transaction monitoring helps detect both **money laundering** and **fraud**. Often integrated software handles AML + Fraud alerts.
10.5.1 Customer-Induced	**Fraud indicators**	Short account lifespan, unusual high-value/fast withdrawals, suspicious funding sources, money mule schemes.

Section	Focus	Key Points
10.5.2 Staff-Related Frauds	**Internal** vulnerabilities	Possible staff red flags: lavish lifestyle, reluctance to take leave, repeated rules violations, etc.
10.5.3 Staff Callousness	**Unintentional** info leaks	Staff training to **avoid** disclosing internal procedures to **outsiders**.
10.5.4 Precautions on New Accts	**Controls** for newly opened accounts	Mark as "new," set system alerts, heightened checks for large transactions, verify instruments dated **before** the account creation.

🗂️ 10.6 MAINTAINING RECORDS 🗂️

🌐 10.6.1 Types of Records

Under **Section 12** of the **PMLA** *(Annexure I)*, banks must **maintain records** of transactions and other customer information. Such records may serve as **evidence** in money laundering cases. **Rules 3 & 4** of the **PML Rules** specify the **types** of records required:

1. **(i) Records of Transactions**
   - 📄 Banks must keep **full** transaction details (allowing **reconstruction** of each transaction).
   - Include transactions **reported** to **FIU-IND** (e.g., **Cash**, **Cross-border**, **Counterfeit Currency**, **Non-Profit Receipts**, **Suspicious Transactions**).

- **RBI** further indicates that **all** background documents, office records, or memos related to suspicious transactions must be retained, with notes from the branch and **Principal Officer**.
- Each transaction record should contain:
  - **Nature** of transaction
  - **Amount & currency**
  - **Date** of the transaction
  - **Parties** involved

2. **(ii) Identity Documents**
   - **PMLA** requires banks to keep records of customer **ID proofs**, including those for **beneficial owners**.
   - **RBI** also instructs retaining **address proofs**.
3. **(iii) Other Documents**
   - **Business correspondence**, account files, client emails, and any communication with **law enforcement** agencies about a customer must be **retained**.
   - **FIU** reports filed by the bank are also part of the **record retention** requirement.

Key Point: Banks should maintain **all relevant records** for **any customer**, regardless of the transaction amount, customer's risk category, or transaction risk.

⏳ 10.6.2 Period of Retention

The **PMLA** stipulates a **5-year** retention period for records, though the **start date** varies by record type:

1. **(i) Transaction Records**
   - **5 years** from the **date of transaction**.
2. **(ii) Identity / KYC Documents**
   - **5 years** from the **later** of:
     - **Cessation of relationship**, **OR**
     - **Closure** of the account.
3. **(iii) Other Documents / Information**
   - **5 years** from the **later** of:
     - **Cessation of relationship**, **OR**
     - **Closure** of the account.

If **legal/regulatory proceedings** are underway or anticipated, **records** must be kept until the matter reaches **final conclusion**.

For instance, where **court cases** are pending, the retention **commences** after the **judgement** date.

💾 10.6.3 Manner of Maintaining Information

Rule 5 of the **PML Rules** states that regulators (e.g., **RBI**) will specify the **form**, **manner**, and **intervals** for record-keeping. **RBI** advises banks to keep records in a **readily accessible** manner, allowing **quick retrieval**. **Hard or soft** format is acceptable, provided they meet these standards.

📝 SUMMARY TABLE

Section	**Focus**	**Key Points**
10.6.1	**Types of Records**	Transaction details (reconstruction), identity docs, and other documents (correspondence, FIU reports, etc.) must be retained.
10.6.2	**Period of Retention**	5 years from transaction date or account closure, depending on the record type. Extended for ongoing legal/regulatory actions.

Section	Focus	Key Points
10.6.3	**Manner of Maintaining**	Records must be easily retrievable. **RBI** allows **hard** or **soft** format, per **Rule 5** of **PML Rules**.