Fraud Monitoring and Reporting Policy 2025-26
Approved by the Board of Directors at its meeting held on29-07-2025, vide Resolution No. 10.

1. Objective

This policy shall be read in conjunction with, and is subject to, the applicable guidelines, circulars, and notifications issued by the Reserve Bank of India (RBI), as amended from time to time. The objective of this policy is to establish a comprehensive and robust framework for the detection, prevention, investigation, and reporting of frauds, in alignment with RBI directives. It is aimed at safeguarding depositors' interests, preserving the financial integrity of the Bank, and maintaining customer trust by ensuring the timely identification, escalation, and mitigation of fraud risks across all operational areas.

2. Definition of Fraud

In accordance with the Reserve Bank of India (RBI) Master Directions on Fraud Reporting, *fraud* is defined as:

"An act of omission or commission by any person, carried out with the intent to deceive, cheat, or cause wrongful gain to one party and/or wrongful loss to the bank or its customers."

Fraud may be perpetrated by internal staff, external parties, or through collusion between both. It covers a wide spectrum of activities that compromise the integrity, security, and financial position of the bank. It includes, but is not limited to, the following:

- **Misappropriation of funds** and **criminal breach of trust** by employees, agents, or third parties
- **Fraudulent encashment** of cheques or instruments using forged signatures, fake documents, or unauthorized access
- **Fabrication or manipulation of records**, including false accounting entries, overstatement or understatement of balances, and misuse of reporting systems
- **Granting or sanctioning of credit facilities** through collusion, kickbacks, or misrepresentation, often for personal or third-party benefit
- **Shortages of cash or securities,** unauthorized withdrawals, or misuse of dormant accounts
- **Cyber frauds, such as:**
    - Phishing, vishing, or spoofing attacks
    - Hacking of banking systems or unauthorized fund transfers
    - ATM frauds, e-mail spoofing, and identity theft
    - Compromise of internal systems or data through malware or ransomware
- **Forging of KYC documents** or misuse of customer credentials
- **Fraudulent bill discounting** or fictitious trade transactions

Fraud also includes willful concealment of material facts, misrepresentation, and breach of contractual obligations with fraudulent intent.

Given the increasing complexity of fraud mechanisms, the Bank must remain vigilant and proactive in implementing strong internal controls, conducting periodic audits, and adhering strictly to RBI's fraud detection, reporting, and monitoring guidelines.
All identified frauds must be reported promptly to the appropriate regulatory authorities, and corrective actions must be taken without delay to prevent recurrence.

---

3. Classification of Frauds

To ensure effective detection, reporting, investigation, and corrective action, frauds shall be systematically classified. The classification is primarily based on the **source** and **nature** of the occurrence. This structured approach helps in identifying systemic weaknesses and formulating preventive strategies.

A. Classification Based on Source / Nature of Occurrence

1. **Advances-related Frauds**
   Frauds associated with loan sanctioning, disbursement, or recovery processes, including:
   - Sanctioning or disbursal of loans based on **forged documents**, **fake identities**, or **inflated asset valuations**
   - **Diversion** or **misutilization** of borrowed funds
   - **Non-compliance** with prescribed credit appraisal or post-disbursement monitoring norms
   - **Fraudulent disposal** or substitution of assets charged to the bank
2. **Deposit-related Frauds**
   Frauds involving manipulation or misappropriation of customer deposits, such as:
   - **Forgery or tampering** of deposit receipts, passbooks, or account statements
   - **Unauthorized withdrawals**, fake transactions, or **impersonation** to access funds
   - **Misappropriation** of proceeds from fixed, recurring, or term deposits
3. **Employee / Staff-related Frauds**
   Frauds committed by internal personnel involving abuse of position or breach of trust, including:
   - Misuse of authority**,** including illegal approvals or collusion with third parties

- Unauthorized system access **or** alteration of records for personal gain
- Theft, bribery, embezzlement**,** or other financial misconduct by employees

4. **Technology-related Frauds**
   Frauds exploiting technology platforms, systems, or digital channels, such as:
   - Hacking or unauthorized access to CBS, internet banking, UPI, IMPS, or mobile banking systems
   - Phishing attacks, malware infections, spoofing, or ransomware incidents
   - Manipulation or misuse of digital banking channels and electronic payment platforms
5. **Third-party / Outsourced-related Frauds**
   Frauds committed by or in collusion with vendors, agents, or outsourced service providers, including:
   - Breach of contract, non-compliance with service level agreements (SLAs), or fraudulent conduct by external partners
   - Collusion between third parties and bank staff to commit fraud
   - Leakage or misuse of confidential data, identity theft, or compromise of outsourced banking services

B. Based on Amount Involved

Frauds shall also be categorized based on the monetary value involved, to determine escalation and reporting procedures:

Category	Amount Range	Action/Reporting Level
Minor Frauds	Below ₹1 lakh	Internal documentation, Board intimation
Significant Frauds	₹1 lakh to ₹1 crore	Report to RBI (CFR Portal), FIR, Audit Committee
Major Frauds	Above ₹1 crore	Report to RBI, Police/CBI, Board-level review

4. Fraud Detection Mechanisms

The Bank shall adopt a multi-layered approach to proactively detect and mitigate fraud risks. The following mechanisms will be implemented to ensure effective monitoring and early identification of fraudulent activities:

- **Regular Internal and Concurrent Audits**
  Routine audits will be conducted to verify compliance with policies, assess internal controls, and identify irregularities in real time.
- **Monitoring of Customer Feedback and Complaints**
  Customer grievances and feedback will be regularly reviewed to detect any signs of fraud or service misuse.
- **System-Generated Alerts**
  The Core Banking System (CBS) and digital banking platforms will generate automated alerts for suspicious or high-risk transactions.
- **Daily Exception Reports and Reconciliation**
  Branches shall generate and review exception reports daily, along with reconciling accounts to identify anomalies or unauthorized transactions.
- **Surprise Inspections and Mystery Shopping**
  Periodic surprise checks and third-party mystery shopping exercises will be conducted to uncover process lapses or fraudulent practices.
- **Whistleblower Mechanism**
  A confidential and anonymous whistleblower framework shall be in place to encourage staff or third parties to report suspected fraud without fear of retaliation.
- **Use of Data Analytics and AI/ML Tools**
  Where feasible, advanced analytics and artificial intelligence/machine learning tools will be deployed to identify patterns, outliers, and potential fraud indicators.

5. Role of Auditors

5.1During the course of the audit, auditors may come across instances where the transactions in the account or the documents point to the possibility of fraudulent transactions in the account. In such a situation, the auditor should immediately bring it to the notice of the senior management and if necessary, to the ACB of the Bank for appropriate action.

5.2 Internal Audit in The Bank shall cover controls and processes involved in prevention, detection, classification, monitoring, reporting, closure and withdrawal of fraud cases, and alsoweaknesses observed inthe critical processes inthe fraud risk management framework of the Bank.

6. Roles and Responsibilities

To ensure effective fraud risk management, the following roles and responsibilities are defined:

- **Branch Managers**
  Act as the first line of defense by detecting, documenting, and promptly reporting any suspicious activities or transactions to the appropriate authorities.
- **Fraud Monitoring Officer (FMO)**
  Serves as the central nodal officer responsible for overall fraud risk monitoring, periodic review of cases, coordination with stakeholders, and timely reporting to regulatory bodies as per RBI guidelines.
- **Audit Department**
  Conducts independent investigations into reported fraud incidents, verifies root causes, and ensures adherence to prescribed regulatory timelines for reporting and closure.
- **Board of Directors / Audit Committee**
  Oversees the review of all major fraud cases, monitors trends and recurring patterns, and ensures implementation of systemic corrective actions to prevent future occurrences

7. Reporting of Frauds to RBI

The Bank shall adhere strictly to the reporting requirements laid down by the Reserve Bank of India (RBI). The timelines and procedures are as follows:

Frauds Involving ₹1 Lakh and Above

- Must be reported to the RBI within **three weeks** of detection through the **Central Fraud Registry (CFR) portal**.

  - Filing of **First Information Report (FIR)** is **mandatory**, and the matter should be reported to the **Police or CBI**, as applicable.
- **Frauds Involving Staff Members**
  - **Mandatory reporting** to both the **RBI** and the appropriate **law enforcement agencies** is required, irrespective of the amount involved.
- **Customer-related Frauds**
  - Must be reported and resolved within the **Turnaround Time (TAT)** prescribed by the **RBI**, ensuring timely communication and redressal.
- **Cyber Frauds**
  - Incidents must be reported to the **RBI within 24 hours** of detection, in line with the provisions of the **RBI's Cyber Security Framework**.

Frauds Below ₹1 Lakh – Explained Simply

- These small frauds do not need to be reported individually to the RBI through the official CFR portal.
- However, the bank will record and investigate them internally as per its own fraud monitoring rules.
- If the fraud involves a bank employee or a customer, the matter must be informed to the Board of Directors, who will decide what disciplinary action to take
- Cyber frauds, even if below ₹1 lakh, must still be reported to the RBI within 24 hours, informed to the Cyber Crime Cell, and all technical records/logs must be saved for investigation.

---

8. Reporting Format and Escalation Matrix

Internal Reporting:

Branch → Fraud Monitoring Officer → CEO

External Reporting:

FMO/Compliance Officer → RBI (CFR portal)

→ Law Enforcement Agency (FIR filing for frauds ≥ ₹1 lakh)

→ DICGC (if deposit insurance claims are involved)

Required Documentation:

- RBI-prescribed fraud report format
- Internal investigation report
- Copies of customer complaints (if applicable)
- Documentary evidence
- FIR copy and follow-up communication

---

9. Customer Communication

In cases where fraud involves customers, the Bank shall follow the protocol below:

- **Notification**: Affected customers shall be informed of the fraud within **7 working days** from the date of detection.
- **Compensation**: Any compensation shall be processed in accordance with the **RBI's Guidelines on Customer Liability in Unauthorized Electronic Banking Transactions**.
- **Awareness**: The Bank shall actively conduct awareness initiatives through:
    - **SMS alerts**
    - **Email notifications**
    - **Updates on the Bank's website**
    - **Educational material displayed at branch premises**

---

10. Monitoring and Review

- The FMO shall submit a quarterly fraud review report to the Audit Committee of the Board
- Frauds involving amounts above ₹1 crore shall be directly reviewed by the Board
- Root cause analysis and necessary systemic corrections will be implemented to avoid recurrence

---

11. Record Keeping

- All fraud-related records, case files, and reports shall be maintained for a minimum of 10 years
- Closed cases shall be archived in both physical and digital formats with appropriate indexing and controls

---

12. Policy Review

This policy shall be reviewed annually or earlier if necessitated by:

- Amendments to RBI guidelines or directives
- Major changes in the Bank's operational, digital, or regulatory environment
- Emerging fraud trends and risk assessment

The Mahaveer Co-operative Bank Ltd., Belagavi

Sd/-

Chief Executive Officer/Vice-Chairman/Chairman