THE MAHAVEER CO-OP. BANK LTD., BELAGAVI

FRAUD MONITORING & REPORTING POLICY

POLICIES FOR THE FY
2026-27
https://mahaveerbank.bank.in

FRAUD MONTORING AND REPORTING 2026-27
WILLFUL DEFAULTER POLICY 2026-27
Approved by the Board of Directors at its meeting held on 23/6/2026**, vide Resolution No.** 11 **.**

➢ Introduction

This policy sets out a clear system for preventing, detecting, classifying, reporting, and monitoring frauds in the Bank, in line with RBI guidelines, the Banking Regulation Act, 1949, and directions issued for Co-operative Banks. Its main aim is to reduce fraud risk, ensure timely and accurate reporting of frauds, and strengthen internal controls to protect the Bank's assets and ensure smooth operations.

➢ Objective

This policy follows the guidelines and instructions issued by the Reserve Bank of India (RBI) from time to time.

- To create a strong system for preventing, detecting, investigating, classifying, and reporting frauds.
- To protect depositors' money and maintain the financial stability of the Bank.
- To build and maintain customer trust by identifying and controlling fraud risks in time.
- To prevent frauds by having strong internal controls and checks.
- To ensure frauds are detected early and reported without delay.
- To bring uniformity in how fraud cases are classified and handled.
- To fix responsibility of staff and take necessary action wherever required.
- To strictly follow RBI rules and timelines for reporting frauds.

➢ Definition of Fraud

Fraud is defined as any act of omission or commission, including misrepresentation, concealment of facts, or abuse of position, committed with the intent to deceive, gain undue advantage, or cause wrongful loss to the Bank, its customers, or any other stakeholder.

1. Misappropriation and Criminal Breach of Trust
- Unauthorized use or diversion of funds or securities entrusted to an employee or third party
- Embezzlement of cash or assets of the Bank

2. Fraudulent Encashment through Forged Instruments
- Encashment of cheques, drafts, or other instruments using forged signatures
- Alteration of financial instruments for wrongful gain

3. Unauthorized Credit Facilities
- Sanction or disbursement of loans without proper appraisal or authority
- Granting advances against fictitious or inadequate securities

- Ever greening or diversion of loan funds

4. Cash Shortages

- Shortage of cash detected during verification
- Theft, burglary, or loss of cash from the Bank's custody

5. Cheating and Forgery

- Opening of accounts with fake documents
- Submission of forged financial statements or identity proofs
- Impersonation for financial transactions

6. Cyber and Digital Frauds

- Internet banking, mobile banking, or UPI-related frauds
- Phishing, vishing, smishing attacks
- Unauthorized electronic fund transfers

7. KYC/Identity Frauds

- Use of fake, stolen, or manipulated identity documents
- Multiple accounts opened using false identities

8. Third-Party / Vendor Frauds

- Fraud committed by outsourced agencies, vendors, or business correspondents
- Manipulation or misuse of systems by service providers

9. Other Frauds

- Any other act not covered above that results in financial loss to the Bank
- Cases involving collusion between employees and external parties

➢ Classification Based on Source of Fraud

Frauds in the Bank shall be classified based on their nature and characteristics, in line with RBI guidelines. The broad categories are as follows:

1. Advances / Loan Related Frauds

- Fraud in sanction, disbursement, or use of loans.
- Use of fake documents, inflated collateral, or diversion of funds.
- Evergreening of loans to hide NPAs.
- **Example:** Loan taken for business but used for personal property purchase.

2. Deposit Related Frauds

- Unauthorized withdrawal or manipulation in deposit accounts.
- Opening accounts using fake KYC documents.
- Tampering with deposit receipts or passbooks.

- **Example:** Fraudulent withdrawal from a customer's FD using forged signature.

3. Staff / Employee Related Frauds

- Fraud committed by employees due to misuse of position.
- Unauthorized transactions, cash misappropriation, or system manipulation.
- Collusion with customers or third parties.
- **Example:** Employee transferring funds from customer account to own account.

4. Technology / Cyber Related Frauds

- Frauds through digital channels like internet banking, UPI, ATM, etc.
- Phishing, hacking, malware, or unauthorized access.
- Data theft or system misuse.
- **Example:** Customer loses money after sharing OTP in a phishing call.

5. Outsourcing / Third-Party Related Frauds

- Fraud by vendors, business correspondents, or service providers.
- Misuse of access, data, or customer information.
- Weak monitoring of outsourced activities.
- **Example:** Business correspondent collecting deposits but not depositing in Bank.

6. Forgery & Documentation Frauds

- Use of fake or altered documents for banking transactions.
- Forged signatures, fake identity proofs, or fabricated financial statements.
- **Example:** Submitting fake income proof to obtain a higher loan.

7. Cash Handling Frauds

- Theft, shortage, or misappropriation of cash.
- Manipulation during cash transactions or vault handling.
- **Example:** Cashier showing less balance than actual cash received.

8. KYC / Identity Related Frauds

- Opening accounts with fake or stolen identities.
- Multiple accounts using false details.

- **Example:** Account opened using another person's Aadhaar for illegal transactions.

➢ Classification of Frauds – Based on Amount Involved

Frauds shall also be classified based on the amount involved for the purpose of reporting, monitoring, and regulatory compliance, as per RBI guidelines:

➢ Small Value Frauds: Below ₹1 lakh

- Involve small amounts and are generally handled at branch level
- Must be recorded and monitored properly
- Reported to RBI in consolidated form as per guidelines

➢ Medium Value Frauds: ₹1 lakh to ₹10 lakh

- Require detailed checking and investigation
- Need timely reporting to higher authorities and RBI
- Closely monitored until closure

➢ Large Value Frauds: Above ₹10 lakh and up to ₹1 crore

- Considered serious and require thorough investigation
- Reviewed by senior management and Audit Committee
- Legal action and recovery steps are initiated

➢ High Value Frauds: Above ₹1 crore

- Have major financial and reputational impact
- Require immediate reporting to RBI (Flash Report)
- Closely monitored by Board and regulators till resolution

This classification shall be used for determining the level of scrutiny, reporting requirements, and escalation to higher authorities, including submission of reports to the Reserve Bank of India (RBI) within prescribed timelines.

➢ Early Warning Signals (EWS)

Early Warning Signals (EWS) are indicators of potential fraud, financial irregularities, or incipient stress in accounts and operations. Timely identification and monitoring of such signals enable the Bank to take preventive and corrective measures to mitigate fraud risk.

The following are illustrative Early Warning Signals:

1. Account Operations Related

- Frequent overdrawing or exceeding sanctioned limits
- Sudden or unexplained changes in transaction patterns
- Large cash transactions inconsistent with the customer profile
- Frequent transfer of funds to unrelated or suspicious accounts

2. Borrowal / Credit Related

- Non-submission or delay in submission of stock statements or financial data
- Significant decline in turnover, sales, or profitability
- Diversion or siphoning of funds
- Frequent restructuring or requests for additional limits without justification
- Irregular repayment or continuous over dues

3. Documentation Related

- Submission of forged, altered, or incomplete documents
- Discrepancies in KYC documents or financial statements
- Non-verifiable collateral or inflated asset valuations

4. Employee Behaviour Related

- Unusual lifestyle or sudden affluence disproportionate to income
- Reluctance to take leave or rotate duties
- Override of internal controls or frequent system exceptions
- Close association with specific customers or vendors

5. Operations / System Related

- Frequent system overrides or backdated entries
- Suspicious reversal or adjustment entries
- Unauthorized access to systems or data
- Repeated audit irregularities

6. Third-Party / Vendor Related

- Unusual payment patterns to vendors
- Lack of proper documentation or agreements
- Complaints regarding service providers

7. Digital / Cyber Related

- Multiple failed login attempts or unauthorized access attempts
- Sudden spike in online transactions
- Reports of phishing, vishing, or unauthorized fund transfers

All identified EWS shall be promptly reported to the Head Office / Fraud Monitoring Cell for further analysis, classification, and necessary action. Continuous monitoring of such signals is essential to prevent potential frauds.

➢ Fraud Risk Governance Structure

The Bank shall put in place a robust Fraud Risk Governance Structure to ensure effective oversight, clear accountability, and timely action for prevention, detection, and reporting of frauds across all levels.

- **Board_of_Directors:**
  Approves the Fraud Risk Management Policy and its periodic revisions, provides strategic direction for fraud risk management, and reviews major fraud cases along with corrective actions
- **Audit_Committee_of_the_Board:**
  Reviews fraud cases above prescribed thresholds, monitors investigation status, evaluates the adequacy of internal controls, and ensures compliance with RBI guidelines and reporting requirements.
- **Chief_Executive_Officer_(CEO):**
  Ensures effective implementation of the policy across the Bank, allocates necessary resources, and oversees timely reporting, investigation, and corrective measures.
- **Branch_Managers:**
  Serve as the first line of defense by ensuring strong internal controls, identifying and reporting Early Warning Signals, and promptly reporting suspected or detected frauds to higher authorities.
- **Employees:**
  Are responsible for adhering to prescribed procedures and ethical standards, promptly reporting suspicious activities, and participating in fraud awareness and training initiatives.

➢ Fraud Detection and Reporting

The Bank shall establish a robust system for timely detection and reporting of frauds to ensure prompt action, regulatory compliance, and mitigation of losses.

- **Detection_of_Fraud:**
  Fraud may be detected through internal controls, audits, inspections, surveillance systems, customer complaints, or identification of Early Warning Signals (EWS). All employees are required to remain vigilant and report any suspicious activity immediately.
- **Immediate_Reporting_by_Branches/Departments:**
  On detection or suspicion of a fraud, the concerned Branch Manager or Department Head shall report

the matter without delay to the Head Office and the Fraud Monitoring Cell (FMC), along with all relevant details and supporting documents.

- **Reporting_to_RBI:**
  The Bank shall report frauds to the Reserve Bank of India (RBI) strictly in accordance with prescribed guidelines and timelines:
    - Flash Report shall be submitted within **24 hours** in cases of frauds involving ₹1 crore and above or as specified by RBI.
    - Detailed Fraud Monitoring Return (FMR) shall be submitted within **3 weeks** from the date of detection.
    - Progress reports and quarterly statements shall be submitted as required.
- **Reporting_to_Law_Enforcement_Agencies:**
  All fraud cases shall be reported to the appropriate law enforcement authorities such as Police/Economic Offences Wing by filing an FIR, without undue delay.
- **Reporting_to_Other_Authorities:**
  Where applicable, frauds shall also be reported to:
    - Registrar of Co-operative Societies
    - Insurance Companies (for claims, if insured)
    - Other regulatory or statutory bodies
- **Confidentiality_and_Documentation:**
  All fraud-related information shall be handled with strict confidentiality. Proper documentation and records of all fraud cases, reports, and correspondence shall be maintained by the Fraud Monitoring Cell.
- **Account_Freezing_and_Preventive_Action:**
  On detection of fraud, immediate steps shall be taken to secure the Bank's interest, including freezing of accounts, blocking of transactions, and preventing further misuse.

This framework ensures early detection, prompt reporting, and compliance with regulatory requirements, thereby minimizing the impact of fraud on the Bank.

➢ Fraud Detection Mechanisms

The Bank shall establish robust and multi-layered fraud detection mechanisms to identify suspicious activities at an early stage and prevent potential losses. These mechanisms shall be integrated across all operational and technological levels.

➢ Internal Control Systems:

- Proper system of checks and approvals is followed for all transactions
- Work is divided among staff to avoid misuse of power
- No single person handles the entire transaction process
  Example: One employee enters a transaction and another verifies and approves it

➢ **Concurrent and Internal Audit:**
- Regular checking of daily transactions and records
- Helps in early detection of mistakes or fraud
- Ensures rules and procedures are properly followed
  Example: Auditor finds unusual repeated entries in a customer account

➢ **Transaction Monitoring through CBS Alerts:**
- CBS system gives alerts for high-value or unusual transactions
- Helps in real-time monitoring of accounts
- Alerts are reviewed by branch officials immediately
  Example: Alert generated for sudden transfer of large amount

➢ **Transaction Monitoring Systems:**
- System tracks customer transaction patterns regularly
- Identifies abnormal or suspicious behavior
- Helps in early detection of fraud trends
  Example: Frequent transfers to unknown accounts are flagged

➢ **Early Warning Signal (EWS) Framework:**
- Identifies early signs of stress or possible fraud
- Monitors loan accounts and customer activities
- Helps in taking preventive action in advance
  Example: Borrower not submitting stock statements on time

➢ **Exception Reports:**
- System generates reports of unusual activities
- Includes limit breaches, overrides, and abnormal entries
- Reports are reviewed regularly by officials
  Example: Account frequently exceeding sanctioned limit

➢ **Surprise Inspections and Cash Verification:**
- inspections without prior notice
- Helps detect cash shortages or irregularities

- Ensures staff follow proper procedures
  Example: Cash found short during surprise branch visit

➢ **Customer Complaints & Feedback:**
- Complaints are treated seriously and checked immediately
- Helps identify unauthorized transactions or fraud
- Quick action prevents further loss
  Example: Customer reports unknown debit from account

➢ **Employee Vigilance:**
- Staff are trained to identify suspicious activities
- Encouraged to report any unusual behavior
- Helps in early detection of fraud
  Example: Employee detects fake documents submitted for loan

➢ **Technology and Cyber Monitoring:**
- Systems monitor online transactions and cyber threats
- Detects hacking, phishing, and unauthorized access
- Ensures safety of digital banking channels
  Example: Multiple failed login attempts detected in net banking

➢ **Reconciliation and Balancing:**
- Regular matching of records and balances
- Identifies errors or missing entries
- Helps in detecting fraud or mistakes
  Example: ATM cash balance not matching system records

➢ **Data Analysis and AI/ML Tools:**
- Advanced tools analyze large data for unusual patterns
- Helps in identifying hidden fraud risks
- Improves accuracy and speed of detection
  Example: System detects same pattern of fraud across many accounts

➢ Reporting Format

1. Internal Reporting

- All suspected or detected frauds shall be immediately reported by the Branch/Department to the Head Office and Fraud Monitoring Cell (FMC).

- The report shall include basic details such as nature of fraud, amount involved, account details, and initial observations.
- Detailed internal reports, including investigation findings, shall be submitted to Senior Management, Audit Committee of the Board (ACB), and Board of Directors, as applicable.
- Periodic status updates on investigation, recovery, and corrective actions shall be shared internally.

2. External Reporting

- Fraud cases shall be reported to the Reserve Bank of India (RBI) as per prescribed formats such as Flash Report and Fraud Monitoring Return (FMR) within stipulated timelines.
- Cases shall also be reported to law enforcement agencies (Police/Economic Offences Wing) by filing an FIR.
- Where applicable, reports shall be submitted to the Registrar of Co-operative Societies and insurance companies.
- Periodic progress reports and quarterly statements shall be submitted to RBI and other authorities as required.

➢ Escalation Matrix

- **Branch/Department_Level:**
  Immediate reporting of suspected/detected fraud to Head Office and Fraud Monitoring Cell (FMC).
- **Head_Office/FMC:**
  Verification, recording, and reporting to RBI and senior management.
- **Senior_Management:**
  Review of significant frauds and monitoring of actions taken.
- **Audit_Committee_of_the_Board:**
  Review of major fraud cases, investigation findings, and control measures.
- **Board_of_Directors:**
  Oversight of major frauds, policy compliance, and strategic decisions.

➢ Legal Action

- The Bank shall initiate legal action in all fraud cases without undue delay.
- An **FIR/complaint** shall be filed with the Police/Economic Offences Wing in respect of fraud cases, as applicable.
- The Bank shall take appropriate legal recourse for recovery of dues through courts, Debt Recovery Tribunal (DRT), or under the **SARFAESI Act**, wherever applicable.

- The Bank shall cooperate fully with law enforcement agencies and provide necessary documents and evidence during investigation.
- Legal proceedings shall be closely monitored until final resolution of the case.
- In cases involving staff, disciplinary and legal action shall be initiated as per service rules and applicable laws.
- The Bank shall also pursue **insurance claims**, wherever applicable, to mitigate losses.

➢ Documentation of Reporting

The following documents shall be maintained for each fraud case:

- Fraud Report (RBI prescribed format – Flash Report / FMR)
- Internal Investigation Report
- Customer Complaint Copy (if any)
- Documentary Evidence (account statements, vouchers, system logs, etc.)
- FIR / Complaint filed with Police or other authorities
- Correspondence with RBI and other regulatory authorities
- Staff accountability / disciplinary action records
- Legal case papers and court proceedings (if any)
- Recovery and insurance claim documents
- Closure report with approval of competent authority

➢ Preventive Measures

- The Bank shall implement strong internal control systems, including segregation of duties and maker-checker mechanisms.
- Proper KYC and due diligence shall be carried out for all customers and transactions.
- Regular internal, concurrent, and statutory audits shall be conducted to identify control gaps.
- Staff shall be trained periodically on fraud prevention, detection, and reporting mechanisms.
- Transaction monitoring systems and alerts shall be used to detect unusual or suspicious activities.
- Access to systems shall be restricted and monitored to prevent unauthorized activities.
- Customer awareness programs shall be conducted to educate them on safe banking practices and fraud risks.
- Timely reconciliation of accounts and verification of records shall be ensured.
- Immediate corrective actions shall be taken on identified weaknesses to prevent recurrence of frauds.

➢ Review of Policy

- This policy shall be reviewed **annually** or earlier, if required, based on changes in RBI guidelines or regulatory requirements.
- Any modifications or amendments to the policy shall be placed before the **Board of Directors** for approval.
- The review shall also consider emerging fraud trends, operational experience, and audit observations.
- The Bank shall ensure that the policy remains updated, effective, and aligned with the latest regulatory and risk management practices.

WILLFUL DEFAULTER POLICY 2026–27

Introduction

This policy is framed in accordance with the Reserve Bank of India (RBI) Master Directions on Wilful Defaulters (latest circulars including July 30, 2024 and subsequent updates). It provides a comprehensive framework for identification, classification, reporting, and monitoring of wilful defaulters.

The policy aims to ensure transparency, fairness, and consistency in dealing with borrowers who deliberately default on their obligations.

Objectives

- To identify borrowers who have the ability to repay but still do not repay the loan
- To prevent misuse or wrong use of Bank funds
- To protect the Bank's money and financial position
- To follow RBI rules and guidelines properly
- To encourage borrowers to repay loans on time and maintain discipline

Definition of Willful Defaulter

A **wilful defaulter** is a borrower who intentionally does not repay the loan despite having the ability to do so, or who misuses the loan funds for purposes other than those approved by the Bank.

A borrower shall be classified as a wilful defaulter in the following cases:

- **Non-repayment_despite_capacity:**
  The borrower has sufficient income or resources to repay the loan but still chooses not to repay.

- **Diversion_of_funds:**
  The loan amount is used for purposes other than what it was sanctioned for. *Example:* Loan taken for business but used for personal expenses.
- **Siphoning_of_funds:**
  The loan funds are used in such a way that they are not traceable or not available for the original purpose.
  Example: Funds transferred to other accounts without proper explanation.
- **Disposal_of_secured_assets:**
  The borrower sells, transfers, or removes the assets given as security without informing the Bank. *Example:* Selling a mortgaged property without Bank approval.

Identification Process

- **Detection_of_Default:**
  The process starts when a borrower fails to repay loan dues on time. Continuous irregularity or non-payment is closely monitored.
- **Examination_of_Account:**
  The borrower's account, transactions, and financial position are carefully reviewed. The Bank checks whether the borrower has the capacity to repay.
- **Verification_of_End_se_of_Funds:**
  The Bank verifies whether the loan amount has been used for the intended purpose. Any diversion or misuse of funds is identified.
- **Collection_of_Evidence:**
  Relevant documents like account statements, audit reports, stock statements, and inspection reports are collected. These help in establishing misuse or intentional default.
- **Assessment_of_Willful_Default:**
  Based on facts and evidence, the Bank examines whether the default is intentional. Cases of diversion, siphoning, or non-repayment despite capacity are considered.
- **Reporting_to_Committee:**
  The case is placed before the Willful Defaulter Identification Committee for review and decision.

Identification Process

- **Detection_of_Default:**
  The process begins when a borrower fails to repay dues on time and the account becomes irregular.

- **Review_of_Account:**
  The Bank examines the borrower's account, financial position, and repayment capacity.
- **Verification_of_End_Use:**
  The Bank checks whether the loan amount has been used for the sanctioned purpose.
- **Collectio_of_Evidence:**
  Relevant documents such as account statements, audit reports, and inspection findings are collected.
- **Assessment_of_Willful_Default:**
  The Bank evaluates whether the default is intentional, including diversion or misuse of funds.
- **Placement_before_Committee:**
  The case is submitted to the Willful Defaulter Identification Committee for decision.

Reporting to RBI and CICs

- The Bank shall report all identified wilful defaulters to **Credit Information Companies (CICs)** such as CIBIL, Equifax, Experian, etc., as per RBI guidelines.
- Reporting shall be done in the **prescribed format** and within the timelines specified by RBI.
- The details reported shall be **accurate, complete, and verified** before submission.
- The Bank shall **regularly update** the status of wilful defaulter accounts, including recovery, settlement, or closure.
- Any **changes or corrections** in the status shall be promptly updated with CICs.
- The Bank shall ensure proper **record maintenance and documentation** for all reported cases.
- Reporting shall be handled by the **designated department at Head Office** to ensure compliance and consistency.

Penal Measures

- No additional credit facilities shall be granted to willful defaulters.
- Existing credit facilities may be **recalled** and recovery action shall be initiated.
- The borrower shall be **debarred from availing finance** from the Bank and other financial institutions.
- Promoters/directors of such entities may also be **restricted from accessing banking finance**.
- Legal action shall be initiated for recovery of dues under applicable laws.
- The Bank may take steps for **enforcement of security** and recovery through SARFAESI/DRT, wherever applicable.
- The name of the willful defaulter shall be reported to **CICs**, affecting their creditworthiness.

Legal Action

- The Bank shall initiate legal action against willful defaulters without delay for recovery of dues.
- Cases shall be filed under applicable laws such as the **SARFAESI Act, DRT, or Civil Courts**.
- An **FIR/complaint** may be filed with Police/Economic Offences Wing in cases involving fraud or criminal activity.
- Action shall also be taken against **guarantors and co-obligants**, wherever applicable.
- The Bank shall take steps for **enforcement and sale of secured assets** to recover outstanding dues.
- All legal cases shall be **closely monitored** until final resolution.
- Proper documentation and records shall be maintained for all legal proceedings.

Dissemination of Information

- The Bank shall share information on willful defaulters with **Credit Information Companies (CICs)** as per RBI guidelines.
- Information may also be shared with **other banks and financial institutions** to prevent further lending to such borrowers.
- Details shall be disclosed only as permitted under **RBI regulations and legal provisions**.
- The Bank shall ensure that all information shared is **accurate, verified, and up to date**.
- Confidentiality shall be maintained, and information shall be shared only with **authorized entities**.
- Wherever required, the Bank may **publish or disclose information** as per regulatory instructions.

Documentation

- The Bank shall maintain proper and complete records for all willful defaulter cases.
- Documents such as **account statements, loan documents, inspection reports, and audit findings** shall be preserved.
- Copies of **Show Cause Notice, borrower replies, and committee decisions** shall be properly maintained.
- Records of **evidence for diversion/siphoning of funds** shall be kept securely.
- All **legal documents, court cases, and recovery actions** shall be documented.
- Reporting records submitted to **RBI and CICs** shall be maintained.
- All documents shall be kept **confidential and preserved** as per regulatory requirements.

Roles and Responsibilities

- **Employees:**

- Follow Bank procedures and maintain proper records
- Remain alert to signs of willful default or misuse of funds
- Report any suspicious cases to higher authorities immediately

- **Branch Manager:**
  - Identify potential willful defaulter cases at branch level
  - Verify account details, end-use of funds, and irregularities
  - Report cases to Head Office with supporting documents
- **Head Office:**
  - Examine and process cases received from branches
  - Place cases before the Willful Defaulter Identification Committee
  - Ensure reporting to RBI/CICs and maintain proper records
- **Audit Committee of the Board (ACB):**
  - Review major willful defaulter cases
  - Monitor compliance with RBI guidelines
  - Ensure proper systems and controls are in place
- **Board of Directors:**
  - Approve the policy and any amendments
  - Provide overall oversight and guidance
  - Review significant cases and ensure proper action is taken

Review of Policy

- This policy shall be reviewed **at least once in a year** or earlier if required.
- Any changes in **RBI guidelines or regulatory requirements** shall be incorporated promptly.
- The review shall consider **practical experience, audit observations, and emerging risks**.
- All amendments shall be placed before the **Board of Directors for approval**.
- The Bank shall ensure the policy remains **updated, effective, and compliant** at all times.

The Mahaveer Co-operative Bank Ltd., Belagavi

Chief Executive Officer/Vice-Chairman/Chairman