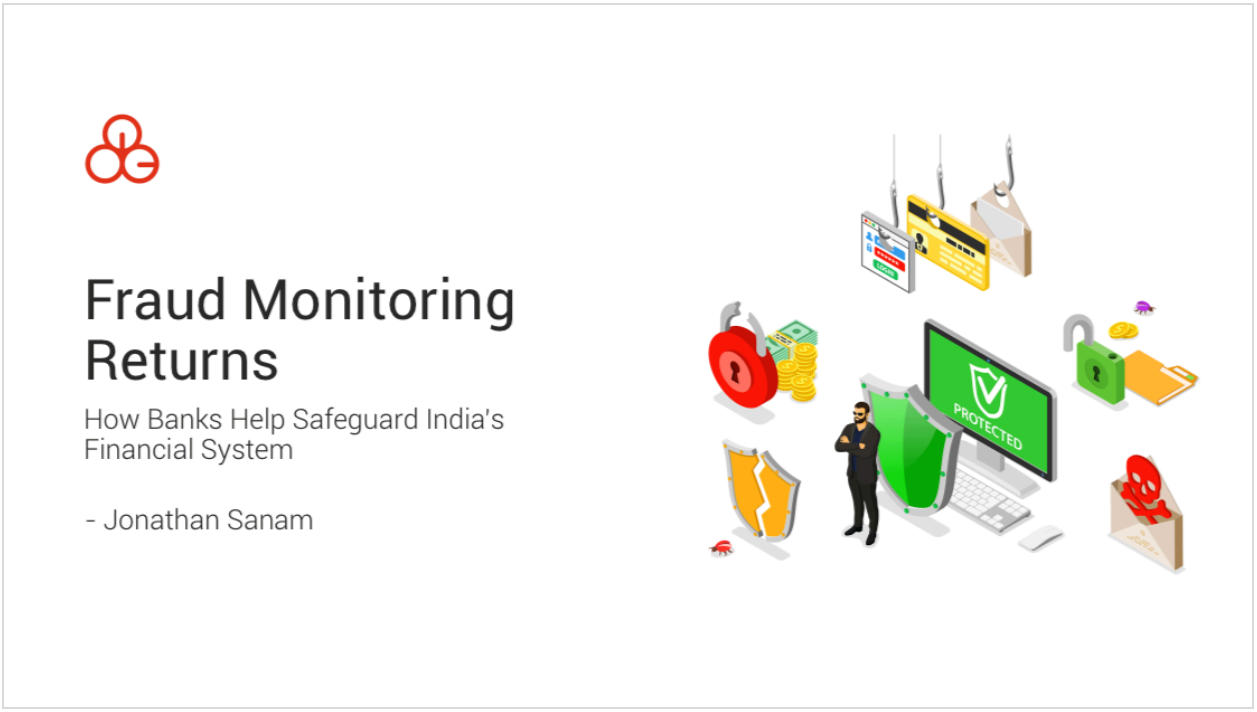


# Fraud Monitoring Returns: How Banks Help Safeguard India’s Financial System

January-4, 2026

According to data released by the Reserve Bank of India (RBI), Digital payment frauds in India saw a fivefold increase to Rs 14.57 billion (Rs 1,457 crore) in FY 2024 from the previous year. RBI data shows that cheap access to the internet along with greater financial inclusion have also led to an increase in digital payments across the country. Digital payments, along with cards and internet transactions, constituted 10.4% of the total fraud amount, up from 1.1% in fiscal 2023. This data highlights the need for stringent fraud regulation to prevent these rising numbers of fraud cases. Fraud Monitoring is the first step in fraud prevention.

Fraud Monitoring

Fraud monitoring is the continuous analysis of user activity, transactions, and data to detect and prevent fraudulent activity in real time. It uses advanced analytics like machine learning and AI, to establish normal behavior patterns and flag anomalies like suspicious transactions or changes to account details. The goal is to identify potential threats in real-time to minimize financial losses and protect customers.

Fraud Monitoring works through:

- Data analysis: Systems continuously monitor a vast amount of data, including transactional activity, user behavior, device information, and IP addresses.
- Behavioral baselines: Machine learning models create a baseline for normal behavior, such as typical spending habits, login times, and locations.
- Anomaly detection: When a user's current activity deviates significantly from their baseline, the system flags it as a potential anomaly.
- Real-time risk scoring: Each session, device, or transaction is given a risk score that updates dynamically as more data is collected, helping to identify potential fraud even if tactics change.
- Intervention: When suspicious activity is detected, the system can trigger an alert for human analysts or automatically implement an intervention, such as requiring additional verification or blocking the transaction entirely.

Fraud Monitoring systems monitor:

- Financial transactions for large purchases, unusual transfer amounts, or frequent transactions.

- User activity for changes to an account's profile, such as adding a new payee or changing contact information.
- Changes in behavioral patterns such as user logging in from a new device or an unusual geographic location.
- Session data to analyze how a user navigates a site, including clicks, swipes, and data entry speed.

Fraud Monitoring is critical because it:

- Reduces financial losses by preventing fraudulent transactions from being completed.
- Protects customers by safeguarding users from having their accounts compromised.
- Maintains brand reputation by protecting the company's image and maintaining customer trust.
- Ensures compliance by helping organizations meet regulatory requirements related to fraud prevention.

Fraud Monitoring Return

One of the regulatory requirements mandated by the RBI for banks and NBFCs in India is the Fraud Monitoring Return (FMR). FMR is a mandatory report submitted by regulated entities like banks and NBFCs to the RBI to report details of fraud incidents. These returns are used to monitor fraud trends, comply with regulations, and provide a detailed report on the nature of the fraud, including the amount, type, and perpetrators.

The purpose of the return is to:

- Inform the RBI about fraud incidents as per its guidelines.
- Classify and track different types of fraud.
- Report on the status of ongoing fraud cases and the closure of those cases.
- Ensure compliance with fraud risk management norms

FMR Reporting requirements

- Reporting threshold: A return must be filed for all frauds of Rs.1 lakh and above.
- Timeline: Returns must be submitted within 14 days of classifying the fraud. A few “Special Reports" have shorter timelines which could be within 7days of classifying the fraud.
- Format: Returns need to be submitted in an electronic/soft copy, which replaces all previous guidelines for hard copy submissions.
- Submission: Reports must be sent to the relevant RBI office, which could be the Central Office, the Central Fraud Monitoring Cell (CFMC) in Mumbai, or a specific Regional Office (RO) depending on the fraud amount and bank's head office jurisdiction.

Key FMR return types: Here are some of the report types used in reporting.

- FMR-1: Is used to report actual or suspected individual fraud cases. Cases involving Rs.1 lakh and above and below Rs.25 lakh are reported to the Regional Office, while cases of Rs. 25 lakh and above are reported to the CFMC in the Central Office.
- FMR-2: Are the fraud details filed of fraud cases that are outstanding at the end of a quarter.

- FMR-3: A quarterly return used to report details of fraud cases that have been closed. This return is cross-checked with FMR-2 and requires prior approval for closure from the relevant Regional Office.
- FMR- 4: Is the report used to file details of burglaries, thefts and robberies.

Responsibility for reporting is usually with a nominated official, often a General Manager, who is responsible for ensuring all fraud returns are submitted correctly and on time.

Key Information included in an FMR are:

- Nature and type of fraud
- Amount involved
- Modus operandi
- Roles of customers, staff, or external parties
- Internal control failures or process gaps
- Steps taken for recovery
- Corrective measures to prevent recurrence

Impact of FMR

How FMRs Help RBI and the banking ecosystem:

- Identify emerging fraud trends
- Flag repeat patterns
- Strengthen supervision
- Support law enforcement when needed

The Bigger Picture - How FMRs Help the Financial Ecosystem

Going beyond mere compliance and the ways that they benefit the banking ecosystem, FMRs help the overall financial ecosystem by:

- Building trust in India's banking system
- Enabling RBI to frame better policies
- Reducing fraud losses across the industry
- Improving customer confidence in digital payments
- Creating a standardized approach to fraud reporting nationwide

Fraud monitoring is no longer just a compliance obligation for Indian banks, it is a *strategic imperative* that protects institutional integrity, sustains customer trust, and supports long-term financial stability. As fraudsters become more sophisticated and technologically enabled, banks must adopt an equally proactive and intelligence-driven approach, integrating advanced analytics, real-time monitoring, and strong internal controls. Looking ahead, the future of fraud risk management in India will be shaped by AI-powered detection systems, greater automation, deeper industry collaboration, and continued regulatory innovation, all of which will enable banks to stay resilient in an evolving threat landscape.


*Quantum Data Engines is a reg-tech company that helps financial institutions detect, manage, and report financial crime more effectively and efficiently.*