



TOUCAN

**Payment Services Operations –
Governance – Fraud Monitoring
& Prevention**



Document History

Date	Version	Prepared by	Reviewed by	Approved by
26 June 2024	1.0	Sastry Lanka	Chakrapani D	Srikanth Mopidevi

Copyright and all rights reserved. No part of this document may be reproduced, stored, or transmitted in any form or by any means, without the prior permission of the Toucan Payments.

Table of Content

1. Governance Framework	3
2. Fraud Risk Categorization	4
3. Fraud Detection Mechanisms	4
4. Fraud Prevention Strategies	5
5. Incident Response and Escalation	6
6. Reporting and Compliance	6
7. Technology and Tools	7
8. Continuous Improvement.....	7
9. Customer Support and Dispute Resolution	7
10. Metrics and Key Performance Indicators (KPIs)	8



1. Governance Framework

A. Fraud Management Committee

- **Composition:**
 - Compliance Officer
 - IT Security Head
 - Representatives from Operations and Customer Support Teams
- **Responsibilities:**
 - Oversee the fraud management strategy and policy implementation.
 - Review and approve new tools and technologies for fraud prevention.
 - Conduct periodic reviews of fraud trends and mitigation measures.
 - Ensure compliance with RBI and regulatory guidelines.

B. Fraud Prevention Policy

- Comprehensive documentation covering:
 - Identification and categorization of fraud risks.
 - Processes for monitoring, investigation, and reporting.
 - Mitigation strategies and escalation procedures.
- Periodic review and updates to align with regulatory and industry changes.



2. Fraud Risk Categorization

Fraud risks are categorized for focused monitoring and mitigation:

- **Merchant-Related Fraud:**
 - Fake or fraudulent merchant accounts.
 - Misuse of payment aggregator services for illegal activities.
- **Transaction Fraud:**
 - Unauthorized transactions using stolen credentials.
 - Phishing or social engineering attacks.
- **Customer Fraud:**
 - Friendly fraud (chargeback fraud).
 - False claims of non-receipt of goods or services.
- **Internal Fraud:**
 - Collusion or misuse of access by employees.
 - System tampering or data leaks.
- **Third-Party Fraud:**
 - Fraud by third-party service providers or partners.
 - Security vulnerabilities in vendor systems.

3. Fraud Detection Mechanisms

A. Real-Time Monitoring

- **Transaction Monitoring:**
 - Monitor key fraud indicators such as velocity checks (number of transactions per user in a defined period) and geographic inconsistencies.
- **Merchant Activity Monitoring:**
 - Analyse merchant behaviour for unusual settlement patterns or chargeback ratios.
 - Conduct random audits of merchant transactions.

B. Rule-Based Systems

- Define pre-set rules for common fraud scenarios, such as:



- High-risk locations (e.g., flagged countries or regions).
- Transactions initiated from suspicious devices or IP addresses.

C. Customer Behaviour Analysis

- Use behavioural biometrics to identify unusual customer actions, such as:
 - Irregular login patterns.
 - Sudden changes in spending habits.

D. Multi-Layer Authentication

- Enforce **multi-factor authentication (MFA)** for all high-value transactions.
- Tokenize sensitive customer data to prevent misuse.

4. Fraud Prevention Strategies

A. Merchant Onboarding

- Conduct stringent due diligence, including:
 - KYC and AML verification.
 - Background checks and validation of business documents.
 - Ongoing monitoring for compliance with terms of service.

B. Customer Awareness

- Regularly educate customers about fraud prevention, covering topics such as:
 - Identifying phishing attempts.
 - Secure password practices.
 - Reporting suspicious activities promptly.

C. Internal Controls

- Implement role-based access controls to restrict sensitive system access.
- Conduct regular employee background checks and training programs.
- Monitor internal system logs for unusual activities.

D. Third-Party Vendor Oversight

- Regularly assess the security and compliance of third-party vendors and partners.



- Include fraud prevention clauses in vendor agreements.

5. Incident Response and Escalation

A. Fraud Detection Workflow

- **Step 1:** Alert triggered by monitoring tools.
- **Step 2:** Initial validation by the Fraud Management Team (FMT).
- **Step 3:** Detailed investigation to assess fraud impact.
- **Step 4:** Immediate action to prevent further losses (e.g., account suspension, blocking suspicious transactions).

B. Escalation Matrix

- Low-impact incidents handled by the FMT.
- High-impact incidents escalated to the Fraud Management Committee.
- Major incidents reported to RBI within prescribed timelines.

6. Reporting and Compliance

A. Regulatory Reporting

- Submit fraud incident reports to RBI in compliance with its guidelines.
- Include details such as the nature of fraud, impact, resolution steps, and preventive measures.

B. Internal Reporting

- Regular reports to the Board of Directors and Risk Management Committee.
- Metrics include:
 - Total fraud attempts and successful prevention rates.
 - Transaction failure rates due to flagged fraud.
 - Trends and patterns in fraud incidents.



7. Technology and Tools

A. Fraud Detection Tools

- **Risk Scoring Engines:** Assign risk scores to transactions based on predefined parameters.

B. Integration with External Databases

- Integrate with NPCI, credit bureaus, and fraud watchlists for enhanced risk assessment.
- Participate in industry information-sharing forums to learn from collective intelligence.

8. Continuous Improvement

A. Post-Incident Analysis

- Conduct root-cause analysis of fraud incidents to identify control gaps.
- Use insights to update fraud detection systems and rules.

B. Periodic Audits

- Conduct quarterly audits of fraud management policies and tools.
- Engage external auditors for unbiased assessment of fraud control effectiveness.

C. Employee Training

- Regularly train employees on fraud detection and prevention best practices.
- Include mock exercises for handling fraud incidents.

9. Customer Support and Dispute Resolution

A. Fraud Reporting Channels

- Provide multiple channels for customers to report suspected fraud, such as:
 - 24/7 hotline.
 - Mobile app or website portal.
 - Email support.

B. Fraud Dispute Process

- Acknowledge customer complaints within **24 hours**.



- Complete fraud investigations within **10 working days**.
- Refund or resolve verified fraud cases as per the liability framework.

10. Metrics and Key Performance Indicators (KPIs)

- **Fraud Detection Rate:** Percentage of fraud attempts successfully identified.
- **False Positives Rate:** Number of legitimate transactions flagged as fraud.
- **Time to Resolution:** Average time taken to investigate and resolve fraud incidents.
- **Customer Satisfaction Score:** Based on feedback from fraud-related complaints.