

# Technical Requirements for Fraud Transaction Monitoring System

---

## 1. Introduction

This document describes the technical and functional requirements for purchasing a fraud transaction monitoring system. Its goal is to provide real-time analysis, detect and prevent fraudulent activities, and ensure compliance with regulations.

---

## 2. Scope

Based on user behavior analysis, the system should monitor transactions from the following channels:

- Internet Banking (internal, national, international transfers).
  - Mobile Banking (internal, national, international transfers).
  - Payments initiated via API.
- 

## 3. Functional Requirements

### 3.1 Real-Time Monitoring

- Process transactions in real time.
- Evaluate and store risk scores based on client behavior.
- Alert management.
- Automatic blocking capability.
- Changing status manually
- Integration with Core Banking system for processed transactions.

### 3.2 Rule-Based Analysis

- Simple visual module for managing rules.
- Logging of customers' historical behavior.
- Logging of deviations from normal behavior.

### 3.3 Reporting and Dashboards

- Dashboards updated in real time.
- Configurable reports.

- Export reports in PDF, Excel, CSV formats.
- Scheduled report delivery.

### **3.4 Integration Capabilities**

- Integration with banking systems.
- Support for industry standards (Recommended JSON)
- Messaging systems (Mandatory RabbitMQ).

### **3.5 Data Storage**

- Access to historical data.
- Access to Audit logs.
- Backup

### **3.6 User & Access Management**

- Role-based access control.

### **3.7 Compliance Requirements**

- Fulfill regulatory requirements.
- 

## **4. Non-Functional Requirements**

### **4.1 Performance**

- Capability to support 200 parallel transactions daily
- Low response time (recommended 50-100ms)

### **4.2 Availability**

- 99.9% SLA.
- 24/7 service and app availability

### **4.3 Security**

- Data encryption. (https protocol, VPN tunnel)
- Protection from OWASP Top 10 threats.
- Secure authorization methods (OAuth2, JWT).

### **4.4 Language and Localization**

- Georgian and English user interface.
  - Support for local time zones and formats.
- 

## **5. Vendor Support**

- 24/7 support.
  - SLA response times.
  - Updates and technical maintenance.
  - Training sessions.
- 

## **6. Implementation Requirements**


- Maximum timeline: 5 months.
  - Detailed implementation plan.
  - Migration of existing data.
  - User Acceptance Testing (UAT) support.
  - Performance and Load Testing.
  - Security Testing.
  - Go-live support.
  - Post-implementation support.
- 

## **7. Documentation**

- User manuals.
  - Administration guides.
  - API documentation.
  - Architectural diagrams.
- 

## **8. Evaluation Criteria**

- Functional compliance.

- 
- Integration capabilities.
  - Price and total cost.
  - Vendor experience.
  - Support conditions.
  - User interface simplicity.
  - Security.