INTELLIGENT FRAUD DETECTION & RISK SCORING SYSTEM

Functional Requirement Document

Business Analyst Project Report
Prepared By: Soundarya S
Role: Business Analyst
Date: October 2025
Version: 1.0

FUNCTIONAL REQUIREMENT DOCUMENT (FRD)

PROJECT: INTELLIGENT FRAUD DETECTION & RISK SCORING SYSTEM

DOMAIN: FINTECH

---

1. Purpose:

This FRD defines the system behaviour, functional rules, data inputs, risk scoring logic, actions, and system flows required to implement an intelligent fraud detection solution that evaluates all transactions in real time.

2. Scope:

- Real-time transaction evaluation
- Risk scoring engine
- Alerts & authentication flows
- Customer fraud reporting
- Fraud Analyst review dashboard
- Error handling & audit logging
- Complaint auto-generation
- Multi-channel notifications

3. Definitions:

Term	Meaning
Risk Score	0–100 risk value assigned to each transaction
High-Risk	Risk score ≥ 80
Very High-Risk	Risk score ≥ 90
Fraud Queue	List of transactions needing analyst review
NFR	Non-Functional Requirements

4. System Overview:

When a customer performs any transaction, the system collects transaction data, applies fraud rules, calculates a risk score, and takes the appropriate automated action based on the risk threshold.

5. Functional Requirements (FR-01 to FR-20):

FR-01: Real-Time Transaction Evaluation

- System must evaluate every transaction within 1 second before approval.

FR-02: Data Capture

System must collect:

- Transaction Amount
- Time/Date
- Device ID
- IP Address
- GPS Location (mobile)
- ATM Location ID (ATM)
- Customer ID
- Previous fraud history

FR-03: Risk Score Calculation

- System must calculate a score from 0–100 using predefined rules.

FR-04: Amount-Based Risk Rule

- ₹50,000 → +20
- ₹1,00,000 → +40

FR-05: Location Mismatch Rule

- If new location differs by >100 km from last known → +20

FR-06: International Location Rule

- If IP or GPS is outside India → +30

FR-07: Device Mismatch Rule

- If new/unregistered device → +25

FR-08: Time-of-Day Risk Rule

- If transaction occurs 12 AM–4 AM → +15

FR-09: High Frequency / Velocity Rule

- If >3 transactions within 1 minute → +25

FR-10: Fraud History Rule

- If customer has past fraud complaints → +30

FR-11: Risk Threshold Actions

- Low Risk (0–59): Auto-approve
- Medium Risk (60–79): Approve + alert
- High Risk (80–89): Hold → OTP/FaceID → approve/reject
- Very High Risk (≥90): Block → alert → fraud queue

FR-12: OTP / Face ID Authentication

- System must trigger OTP/Face ID when risk score is 80–89.

FR-13: Customer Alerts

System must send SMS/Email/Push for:

- Medium Risk
- High Risk
- Blocked transactions

FR-14: Customer "Not Me" Action

If user clicks "NOT ME":

- Block card instantly
- Stop all outgoing transactions
- Generate fraud complaint
- Notify Fraud Analyst

FR-15: Fraud Queue

System must send flagged transactions to queue with:

- Reason code
- Risk score
- Location
- Device
- Customer history

FR-16: Complaint Auto-Generation

- Each fraud report must auto-create a complaint with unique ID.

FR-17: Error Logging

- System must log all errors with timestamp, device ID, IP, exception message.

FR-18: Error-Based Escalation

- If error occurs during a suspicious (≥80 risk) transaction → escalate to Fraud Analyst.

FR-19: Audit Trail

- Track every action: OTP fails, approvals, rejections, alerts sent, device mismatch, etc.

FR-20: Fraud Dashboard

Dashboard should show:

- Total flagged transactions
- High-risk cases per hour
- OTP success/failure
- "Not Me" reports
- Fraud resolved cases

6. Risk Scoring Logic Table:

Condition	Score
Amount > ₹50,000	+20
Amount > ₹1,00,000	+40
New Device	+25
Location >100 km	+20
International IP	+30
Time 12AM–4AM	+15
>3 transactions/min	+25
Past fraud history	+30
Wrong OTP attempts (3)	+10

Final Risk Score = Sum of triggered rules (Max 100)

7. System Decision Flow:

Low Risk (0–59)

- Approve
- No OTP
- No review

Medium Risk (60–79)

- Approve
- Send warning alert

High Risk (80–89)

- Hold transaction

OTP / FaceID required

- If success → approve
- If fail → block

Very High Risk (≥90)

- Block
- Send alert

Send to Fraud Queue

Auto-generate complaint

8. Exception Handling:

- Missing GPS → require OTP
- SMS not delivered → retry 3 times
- OTP server down → block high-risk transactions
- Location mismatched + new device + large amount → instant block

9. Data Requirements:

Field	Description	Type
transaction_id	Unique ID	String
customer_id	Customer unique ID	String
Amount	Transaction amount	Decimal

device_id	Device identifier	String
ip_address	IP address	String
gps_location	Lat/Long	String
atm_location_id	ATM branch code	String
risk_score	Calculated score	Integer
flag_reason	Reason for risk	String

10. Integration Requirements:

- SMS Gateway API
- Email API
- Push Notification API
- Face ID/OTP Auth API
- Fraud Complaints API
- Core Banking API
- Dashboard API

11. NFR (Non-Functional Requirements):

NFR	Requirement
Performance	Risk scoring < 1 sec
Scalability	10,000 transactions/min
Availability	99.9% uptime
Security	AES-256 encryption
Compliance	Must meet RBI fraud guidelines

Logging All actions logged

12. Acceptance Criteria (High-Level):

- System blocks all transactions with risk ≥ 90
- OTP must trigger for risk 80–89
- Alerts delivered within 5 seconds
- Risk score must update dashboard instantly
- Fraud Queue must refresh in real time
- “Not Me” must block card immediately