**Business Requirements Document (BRD)**

**Project: AI/ML-Based Fraud Detection System**

**Client:** Titan National Bank  
**Date:** June 30, 2025  
**Prepared by:** Enterprise Data Science & Risk Team

**1. Executive Summary**

Titan National Bank aims to implement an AI/ML-driven fraud detection system to reduce financial losses and operational risk caused by fraudulent transactions across digital and branch channels. The proposed solution will leverage advanced machine learning models to identify and prevent suspicious activity in real time, supporting both automated action and analyst review.

**2. Project Objectives**

* Detect potentially fraudulent transactions in real time with minimal false positives.
* Reduce financial and reputational losses from fraud.
* Provide explainable alerts and actionable insights to compliance teams.
* Improve operational efficiency by automating first-level fraud checks.
* Ensure compliance with local and global regulatory requirements.

**3. Scope of Work**

**In Scope:**

* Ingestion of real-time and batch transaction data from core banking, mobile, and online channels.
* Model training on historical labeled fraud data.
* Real-time scoring API for transactions.
* Alert dashboard for compliance analysts.
* Case management and workflow integration.
* Explainability module for generated alerts.
* Integration with existing transaction monitoring systems.
* Automated blocking and hold functionality for suspicious transactions.
* Periodic model retraining and performance monitoring.
* Integration with notification/email systems for critical alerts.

**Out of Scope:**

* End-customer-facing fraud notification.
* Fraud detection for credit card issuance (focus is on account transactions).
* On-premise deployment (cloud-only in this phase).

**4. Functional Requirements**

**4.1 Data Integration**

* Support real-time ingestion of transactions via API (max latency 500ms).
* Batch data load for historical transactions (daily, nightly).
* Data enrichment using customer profiles, geo-location, device metadata, etc.
* Ingest third-party data feeds (blacklists, AML watchlists).

**4.2 Model Training & Scoring**

* Train supervised ML models (e.g., XGBoost, neural nets) using labeled data (fraud/no-fraud).
* Support for feature engineering and selection workflows.
* Store model versioning and lineage.
* Real-time model scoring endpoint (REST API) with <300ms average response time.
* Output fraud risk score (0-1), risk category, and key contributing features.

**4.3 Alert Generation & Workflow**

* Auto-generate alerts for all high-risk transactions (score > threshold).
* Present alerts in analyst dashboard with transaction details, risk score, and explanation.
* Analyst can accept, reject, or escalate alerts.
* Link alert cases to customer master profile.
* Support bulk operations for low-risk batch dismissals.

**4.4 Case Management**

* Assign cases to analysts based on workload and expertise.
* Log analyst actions with timestamp and user ID.
* Support for multi-level approval workflow.
* Integration with internal case management system.

**4.5 Explainability**

* Display top features contributing to fraud score for each alert.
* Provide plain-language reason codes for flagged transactions.
* Support export of alert explanation for audit purposes.

**4.6 Integration & Automation**

* Webhooks or APIs to trigger account hold/block automatically.
* Integration with SMS/email systems for compliance notifications.
* API endpoints for updating thresholds and model configurations.

**5. Non-Functional Requirements**

* System uptime: 99.9% (24x7 operation)
* Average scoring API response time: <300ms
* Scalable to 10,000 TPS (transactions per second) during peak
* Data encryption at rest and in transit
* Role-based access control for dashboards and APIs
* Audit logs for all actions and model decisions
* GDPR and local regulatory compliance (data residency, right to explanation)
* Modular and containerized architecture (Docker/Kubernetes-ready)
* Disaster recovery: RPO 15 min, RTO 2 hours

**6. Compliance & Security**

* Must comply with RBI, SEBI, and global banking regulations on fraud detection and reporting.
* Periodic independent security and compliance audits.
* Masking of PII in logs and exports.
* Only authorized compliance/IT staff can access full transaction details.

**7. Dependencies**

* Access to core banking transaction systems and APIs.
* Integration with existing customer master data and AML systems.
* Secure access to historical labeled fraud data.
* Availability of compliance and IT support for integration.

**8. Risks & Assumptions**

* Timely access to labeled historical fraud data.
* Regulatory approvals for storing and processing customer data in the cloud.
* User acceptance and training for new dashboards and workflows.
* Model drift and changing fraud patterns requiring regular retraining.

**9. Acceptance Criteria**

* At least 85% detection rate on historic fraud cases (recall) with <2% false positive rate.
* Real-time scoring latency <300ms for 99% of requests.
* All alerts must include clear explanation and supporting details.
* Successful end-to-end UAT with compliance and IT sign-off.
* Complete audit log for every decision and alert.

**10. Stakeholders**

* Project Sponsor: Chief Risk Officer
* Product Owner: Head of Fraud Analytics
* Compliance Team Lead
* IT Integration Manager
* End Users: Fraud analysts, compliance team