Fraud Risk Analytics & Behavioral Anomaly Detection

1-Page Analytics Case Study

Problem Statement

Digital payment systems process millions of transactions daily, where **fraud events are rare but financially severe**.
Risk teams face three key challenges:

- Extreme **class imbalance** (fraud < 1%)
- High **manual investigation costs**
- Lack of **prioritization** in fraud alerts

The objective was to build an **explainable analytics solution** that helps **identify high-risk transactions and prioritize investigations**, rather than relying on black-box predictions.

Dataset Snapshot

- **Total Transactions:** ~6,000,000
- **Fraud Transactions:** 8,213
- **Fraud Rate:** 0.13%
- **High-Risk Transactions Identified:** 954

This reflects a **realistic BFSI fraud environment** with sparse fraud occurrences.

Approach & Methodology

1. SQL-Based Feature Engineering

Engineered interpretable fraud risk signals using SQL:

- Balance mismatch detection
- Extreme transaction amount flags (statistical thresholds)
- Sender-level behavioral baselines
- Time-based behavioral deviation analysis

SQL techniques used:
CTEs, window functions, aggregations, behavioral metrics

---

2. Risk Scoring Framework

Designed a **risk score (0–1)** per transaction by combining:

- System fraud flags
- Amount anomalies
- Balance inconsistencies
- Behavioral deviations

This enabled **risk prioritization** instead of binary fraud classification.

---

3. Power BI Fraud Monitoring Dashboard

Built a multi-page dashboard aligned with **real fraud operations workflows**:

Executive Overview

- Transaction volume
- Fraud rate
- Trend monitoring

Fraud Pattern Analysis

- Fraud rate by transaction type
- Amount bucket risk analysis
- Behavioral indicators

High-Risk Transaction Queue

- Analyst-ready investigation table
- Risk score–based filtering
- Actionable review interface

Key Insights

- Fraud is **highly concentrated**, with a small subset of users driving most fraud
- Certain transaction types show **significantly higher fraud rates**
- High-value and anomalous transactions exhibit elevated risk
- Behavioral deviation is a stronger indicator than transaction count
- Fraud events show **temporal clustering**, indicating attack windows

---

Business Impact & Recommendations

- Enable **risk-based prioritization** to reduce analyst workload
- Auto-flag transactions with **risk score > 0.85**
- Increase monitoring on **high-value transfer transactions**
- Focus controls on repeat behavioral anomalies rather than volume alone

---

Tools & Skills Demonstrated

- **SQL (MySQL):** Feature engineering, window functions, behavioral analysis
- **Power BI:** KPIs, slicers, analyst dashboards
- **Fraud & Risk Analytics:** Imbalanced data handling, prioritization
- **Business Analytics:** Insight generation and decision support

---

Why This Project Matters

This project mirrors **real-world fraud analytics systems**, where the goal is not just detection, but **explainability, prioritization, and actionability** for risk teams.