Digital Payments Fraud Risk & Internal Control Analytics Report

1. Executive Summary

This project evaluates fraud risk and internal control effectiveness within a simulated digital payments environment using transaction-level data from the PaySim dataset. A rule-based fraud risk engine was developed to identify high-risk transactions using interpretable audit logic. The model's effectiveness was compared against the system's built-in fraud detection flag to assess control performance.

The analysis highlights fraud concentration in specific transaction types and identifies balance validation inconsistencies as a key risk indicator. The results support a risk-based audit approach for prioritizing transaction review.

2. Objective

The objective of this project was to:

- Identify fraud patterns in digital payment transactions
- Detect anomalies and exceptions using rule-based analytics
- Evaluate the effectiveness of existing fraud detection controls
- Develop a risk scoring model to support audit planning
- Create a management-level dashboard for continuous monitoring

3. Dataset Overview

- Dataset: PaySim Mobile Money Fraud Simulation
- Sample Size: 300,000 transactions
- Total Variables: 11
- Fraud Label: `isFraud` (1 = Fraud, 0 = Non-Fraud)
- System Flag: `isFlaggedFraud`

Key Variables Used:

- `type` (Transaction category)
- `amount` (Transaction value)

- `oldbalanceOrg`, `newbalanceOrig`
- `oldbalanceDest`, `newbalanceDest`

The dataset is highly imbalanced, with fraud representing a very small percentage of total transactions. This mirrors real-world financial fraud scenarios.

4. Methodology

A rule-based fraud risk engine was developed using four core audit rules:

Rule 1 — Balance Validation Check

Transactions were flagged if the sender's post-transaction balance did not reconcile with the expected balance calculation.

Rule 2 — High-Value Transaction Flag

Transactions above the 99th percentile threshold were classified as high-risk.

Rule 3 — High-Risk Transaction Type

Transactions categorized as TRANSFER and CASH_OUT were flagged due to observed fraud concentration.

Rule 4 — High-Frequency Customer Behavior

Senders with unusually high transaction counts were flagged as behaviorally suspicious.

5. Risk Scoring Model

A weighted risk score was calculated as:

- Balance mismatch → Weight 3
- High-value transaction → Weight 2
- High-risk type → Weight 2
- High-frequency sender → Weight 1

Transactions with a score ≥ 4 were classified as High Risk.

This risk-based approach supports transaction prioritization for audit review.

6. Analytical Findings

6.1 Fraud Concentration by Process

Fraud cases were predominantly concentrated in:

- TRANSFER transactions
- CASH_OUT transactions

These processes represent higher inherent fraud risk and require stronger monitoring controls.

6.2 Balance Validation Weakness

A significant proportion of fraudulent transactions exhibited balance inconsistencies. This suggests potential weaknesses in transaction validation logic and highlights a control design gap.

6.3 Model vs System Detection

The system's built-in fraud flag (`isFlaggedFraud`) detected only a portion of total fraud cases.

The rule-based risk model:

- Improved fraud prioritization
- Captured a higher percentage of fraud in high-risk transactions
- Provided interpretable detection logic

This demonstrates that additional audit-layer analytics can enhance fraud monitoring effectiveness.

7. Control Effectiveness Assessment

The following control issues were observed:

- False negatives: Fraud transactions not flagged by the system
- Over-reliance on static detection thresholds
- Insufficient behavioral monitoring

The system detection mechanism may benefit from enhanced anomaly detection logic.

8. Dashboard Implementation

A corporate-style Power BI dashboard was developed with three layers:

Executive Overview

- Total Transactions
- Total Fraud
- Fraud Rate
- High-Risk Transactions

Process-Level Analysis

- Fraud concentration by transaction type
- Fraud rate by process

Control Effectiveness

- System detection performance
- Risk model detection comparison
- Balance mismatch impact

The dashboard supports data-driven audit planning and continuous monitoring.

9. Recommendations

1. Strengthen monitoring of TRANSFER and CASH_OUT transactions
2. Improve balance validation controls to reduce inconsistencies
3. Introduce behavior-based anomaly detection
4. Periodically recalibrate fraud detection thresholds
5. Use risk-based prioritization for transaction audits

10. Limitations

- Dataset is simulated, not real banking data
- No demographic or customer segmentation data available
- Rule-based models may generate false positives
- Machine learning enhancements were not implemented in this phase

11. Conclusion

This project demonstrates how rule-based analytics can enhance fraud detection and internal control evaluation in digital payment systems. By combining anomaly detection, process-level analysis, and risk scoring, the solution supports efficient audit planning and improved fraud monitoring.

The approach aligns with internal audit objectives by prioritizing high-risk transactions, evaluating control effectiveness, and enabling management reporting through interactive dashboards.