Users Churn & Fraud Monitoring Dashboard

Project Objective

The primary goal of this project was to identify and understand user churn behavior as well as uncover suspicious or potentially fraudulent transactions. The churn analysis focuses on users who have stopped transacting over a period of time, while the fraud analysis aims to flag unusually large transactions for further investigation. The ultimate aim is to support reactivation strategies and enable early fraud detection.

1. Churn Analysis

- Total users in the dataset: 280

- Total number of transactions: 1,000

- Churn rate: 30% (users inactive for 90+ days)

- Active user rate: 70%

- Average days since last transaction (for churned users): 153 days

Monthly churn trends show a significant spike in May (36%), followed by another high in September. The lowest churn was recorded in June. A rising churn rate is a negative signal, and a drop indicates improvement.

User Attributes of Churned Users

- 68% of churned users had successful transactions, suggesting the churn is not due to failed experience or app issues.

- 80% of churned users are verified indicating they were properly onboarded and not casual users.

- South Africa had the highest number of churned users, followed by Ghana, Kenya, Uganda, and Nigeria.

- 59% of churned users had a card linked; 41% did not, implying a potential lack of commitment.

- Most churned users are on Tier 1 accounts, while Tier 3 users (more invested) churn less.

Recommendations to Reduce Churn

- Run reactivation campaigns (email, SMS) targeting Tier 1 and unlinked users.

- Issue ATM cards on signup to increase attachment to the app.

- Expand language options in-app to improve retention in South Africa and other key regions.

• Incentivize users to upgrade to higher tiers (e.g. through benefits, discounts, or limits).

2. Fraud & Anomaly Detection

• Flagged transaction rate: 24.3% of all transactions

• Total flagged transaction volume: $4.2 million

• Total overall transaction volume: $6.2 million

• Volume flagged as suspicious: 67.45% — a major red flag

The high flagged percentage indicates that while suspicious transactions are few in count, the amounts involved are large. Spikes in flagged transaction amounts were observed in August and September (e.g., ~$639K), followed by a drop in October and subsequent increase in November and December.

Fraud by Dimensions

• By country: South Africa leads, followed by Uganda, Kenya, Ghana, and Nigeria.

• By status: 76% of flagged transactions were successful — this implies that most high-value transactions went through without blockage.

• By channel: USSD (38%) was the most used method for flagged transactions, followed by web (33%) and mobile (30%).

Flagged Users Table

A detailed table of suspicious transactions allows for further drill-down into users, recipients, and timestamps. These can be cross-checked with the backend for audit or AML procedures.

Churned Users Linked to Suspicious Activity

An additional observation from the analysis reveals that approximately 34% of the users who have churned also appear in the suspicious fraud table. This overlap is significant, as it may indicate a pattern where users associated with high-value or suspicious transactions later disengage from the platform. While this does not confirm fraudulent intent, it does suggest the need for closer monitoring of such users both to mitigate financial risk and to understand possible reasons for disengagement.

Recommendations for Fraud Mitigation

• Set automated red flags for transactions above a threshold with real-time checks.

• Introduce stepped verification: suspicious amounts must go through security questions or OTP re-confirmation.

• Review all flagged users periodically and audit activity pre- and post-churn.

- Invest in user education and stricter onboarding compliance — especially in high-flag regions like South Africa.