FINTECH PAYMENT TRANSACTION ANALYTICS

Fraud Intelligence Dashboard — Documentation

1. Project Objective

Design a single-page fintech fraud intelligence dashboard that provides clear visibility into transaction growth, fraud exposure, and risk concentration across countries, merchant categories, and payment channels, using structured analytics and machine-learning-assisted risk signals.

2. Key Business Questions

- How does transaction volume evolve over time?
- How is fraud exposure distributed across countries?
- Which merchant categories consistently show higher fraud risk?
- How do payment channels and card providers influence transaction exposure?
- Where should fraud monitoring efforts be prioritized?

3. Dashboard Insights

3.1 Transaction Volume Trend

- Transaction volume demonstrates strong but volatile growth across the year. Activity dips noticeably around mid-year (June) before recovering and trending upward toward year-end.
- **Interpretation:**
  This pattern suggests fluctuating transaction behavior, potentially driven by seasonal effects, user activity cycles, or operational factors. While growth is evident, volume instability highlights the need for continuous monitoring rather than point-in-time analysis.

3.2 Country-Level Fraud Exposure

- Fraud exposure across countries shows only slight variation, with most values clustering closely together.
- Uganda and Ghana exhibit the highest relative fraud exposure.
- South Africa and Nigeria follow closely, despite having different transaction volumes.
- Kenya maintains comparatively lower fraud exposure.
- Implication:
  Fraud risk is broadly distributed rather than concentrated in a single market. This suggests that fraud controls should be country-aware but consistently applied, rather than heavily skewed toward one geography.

3.3 Fraud vs Legitimate Transaction Mix

- Legitimate transactions remain the majority, while fraudulent transactions represent a smaller but persistent share of overall activity.
- Interpretation:
  Although fraud is not dominant by volume, its presence across multiple segments reinforces the importance of early detection and continuous risk scoring rather than reactive investigation.

3.4 High-Risk Merchant Categories

- Consistently elevated fraud concentration is observed across the following merchant categories:
- Airtime/Data
- Bills Payment
- E-commerce

- Food Delivery
- Professional Services
- These categories cluster around ~10% or higher fraud exposure, indicating structural rather than incidental risk.

Implication:

Merchant category is a strong risk indicator. Targeted controls, monitoring thresholds, and enhanced verification should be prioritized for these segments.

3.5 Card Provider & Payment Channel Exposure

- Card-based transactions are prominent due to the presence of multiple card providers in the dataset.
- Visa and Mastercard account for the majority of card usage.
- A significant share of transactions occurs without card usage, with wallet and transfer-based channels recording the highest transaction volume overall.

Implication:

While card transactions remain important, non-card payment channels drive the largest volume, making them critical to fraud monitoring and operational oversight.

3.6 Fraud Trend Context

Fraud exposure remains relatively controlled across segments, but its consistent presence across time, countries, and categories highlights the importance of proactive monitoring rather than threshold-based reactions.

4. Business Recommendations

Area	Recommendation
Transaction Monitoring	Track volatility and growth trends continuously, not just total volume
Country Risk	Apply uniform fraud frameworks with country-level tuning
Merchant Controls	Prioritize high-risk categories for enhanced validation and review
Payment Channels	Expand fraud monitoring beyond cards to wallet and transfer channels
Risk Strategy	Shift from static labels to early risk signals and trend detection
Reporting	Maintain a single-page executive dashboard for fast decision-making

5. Role of Machine Learning

- Machine learning supports analysis without replacing human judgment:
- Pseudo-labeling simulates fraud indicators
- Models highlight risk patterns across transactions
- Explainability techniques validate feature influence
- Outputs feed dashboard insights, not automated blocking

6. Why This Project Matters

- This project demonstrates:
- Strong alignment between business questions and analytics output
- Practical fraud intelligence design
- Clean, executive-ready Power BI storytelling
- Thoughtful use of machine learning for decision support

- Portfolio-quality documentation suitable for real-world fintech use cases

Final Note

This dashboard provides a clear, balanced view of growth and risk within a fintech transaction ecosystem. It emphasizes clarity, proportional risk assessment, and scalable monitoring, making it ideal for stakeholder communication, portfolio presentation, and technical interviews.