Fraud Detection in Digital Wallet Transactions

Leveraging Data to Identify High-Risk Transactions

Presenting:
Aaron Marshall
Ashleigh Clark

Problem Statement & Significance

- Problem: Fraud in digital wallet transactions poses significant risks to consumers and businesses.
- Significance:
  - **Growing** adoption of digital payments increases vulnerability.
  - Fraud impacts financial trust, causing financial losses and operational insights.
- Objective: Develop methods to flag suspicious transactions using data-driven insights.

Data Collection

- Data Source: Synthetic dataset from **Kaggle**, representing digital wallet transactions
- **Why This Dataset?**:
  - Detailed transaction-level data, including timestamps, locations, and payment methods
  - Suitable for developing fraud detection techniques
- Data Attributes:
  - Key fields: transaction amount, user location, product category, payment method.

Data Processing & Challenges

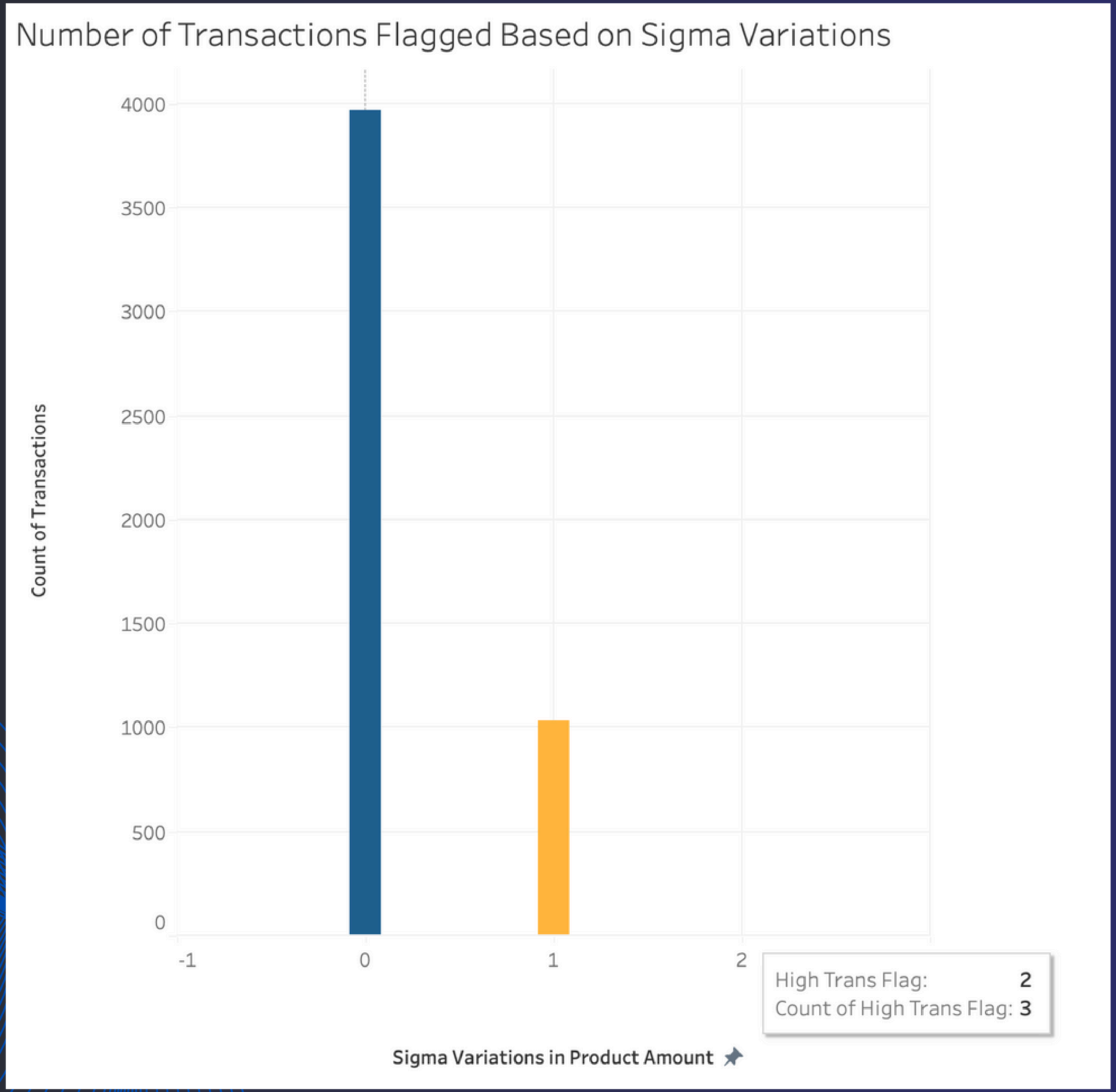
- Approach:
  1. Data Cleaning
  2. Feature Engineering [Fraud Indicators]
     - High Transaction Amounts
     - Unusual Location for User's Transactions
     - Unusual Payment Methods
  3. Data Aggregation
- Key Challenges:
  - Managing inconsistencies
  - Deciding appropriate thresholds
- Solution: Iterative refinement of indicators based on **feedback and exploratory analysis.**

Fraud Detection Analysis

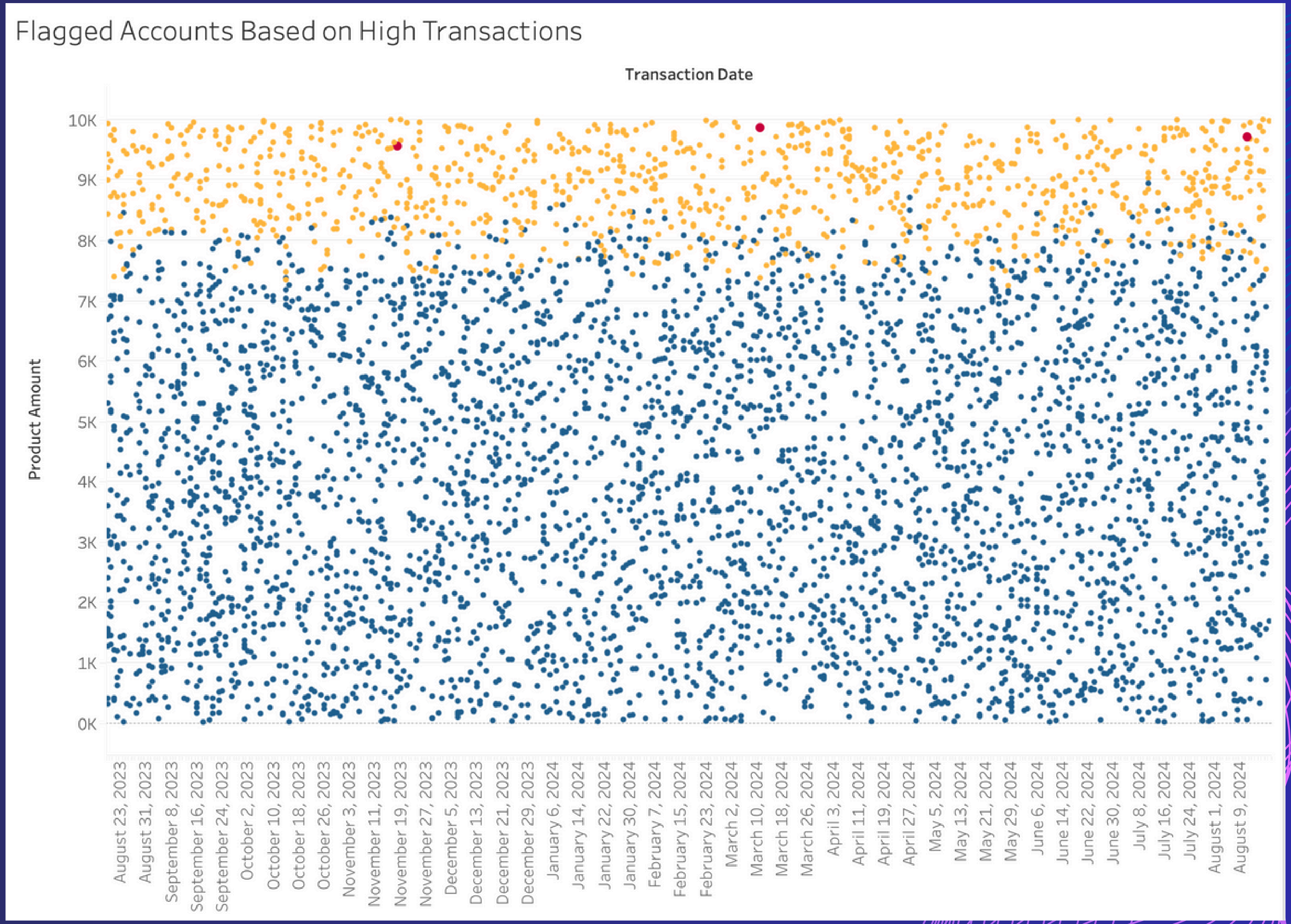
Indicator 1: High Transaction Amounts

- Use the average and standard deviations of product amounts to develop a baseline for typical amounts of transactions
    - To provide more accurate baselines, calculate average and standard deviations per product
- Evaluate multiple sigma values to determine which is the most insightful
- This indicator focuses on all the transaction data as a whole to determine baseline (does not depend on each user’s individual history)

Indicator 1: High Transaction Amounts



Number of Transactions Flagged Based on Sigma Variations

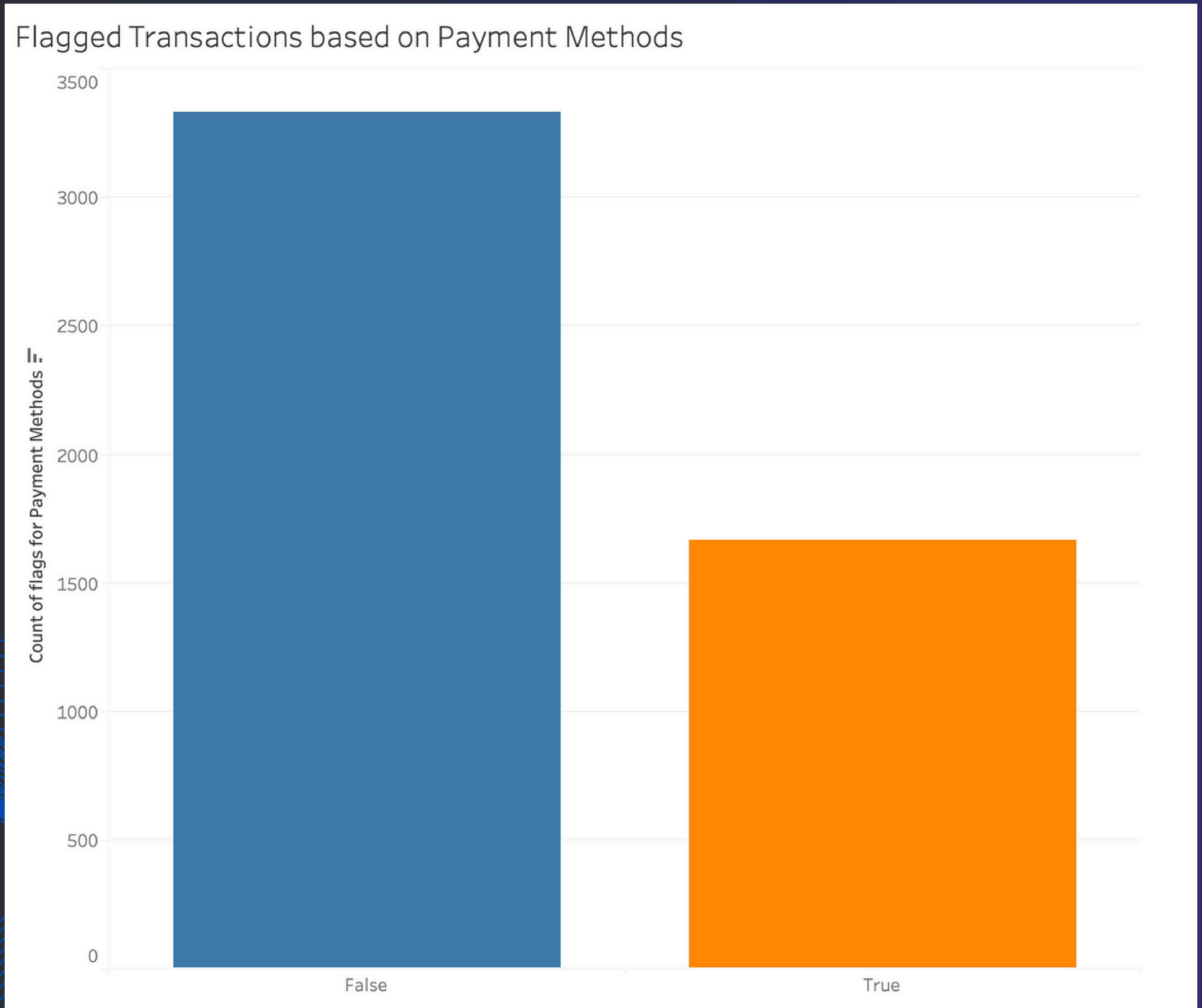


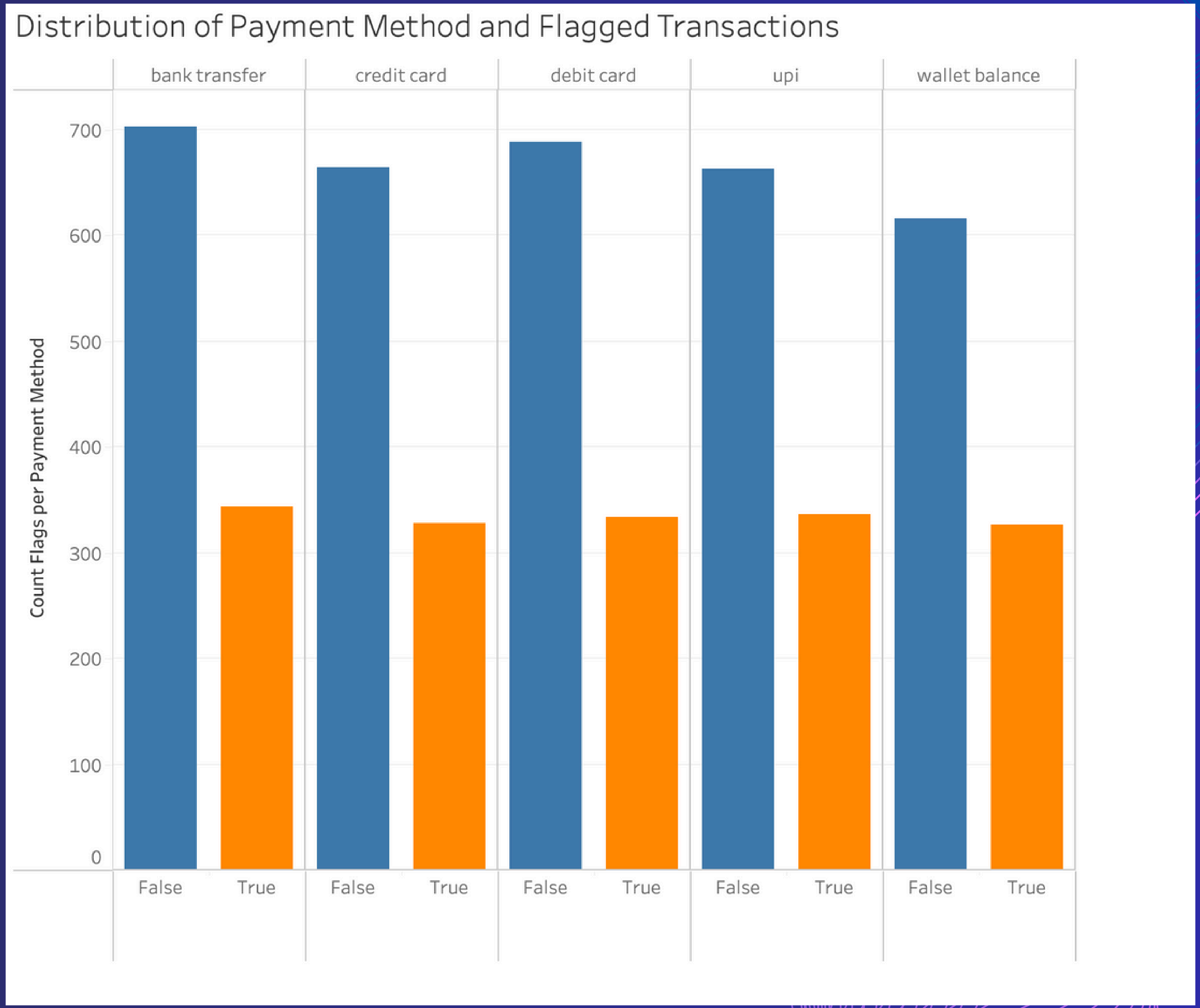
Flagged Accounts Based on High Transactions

Indicator 2: Unusal Payment Methods

- Focuses on each user's history to evaluate transactions that use a nontypical payment method
- Based on history, flags transactions that use a different payment method than previously determined
- Opportunity to allow for more than one payment method based on user history
  - Indicator is easily adjusted to account for multiple payment methods commonly used if indicated

Indicator 2: Unusal Payment Methods

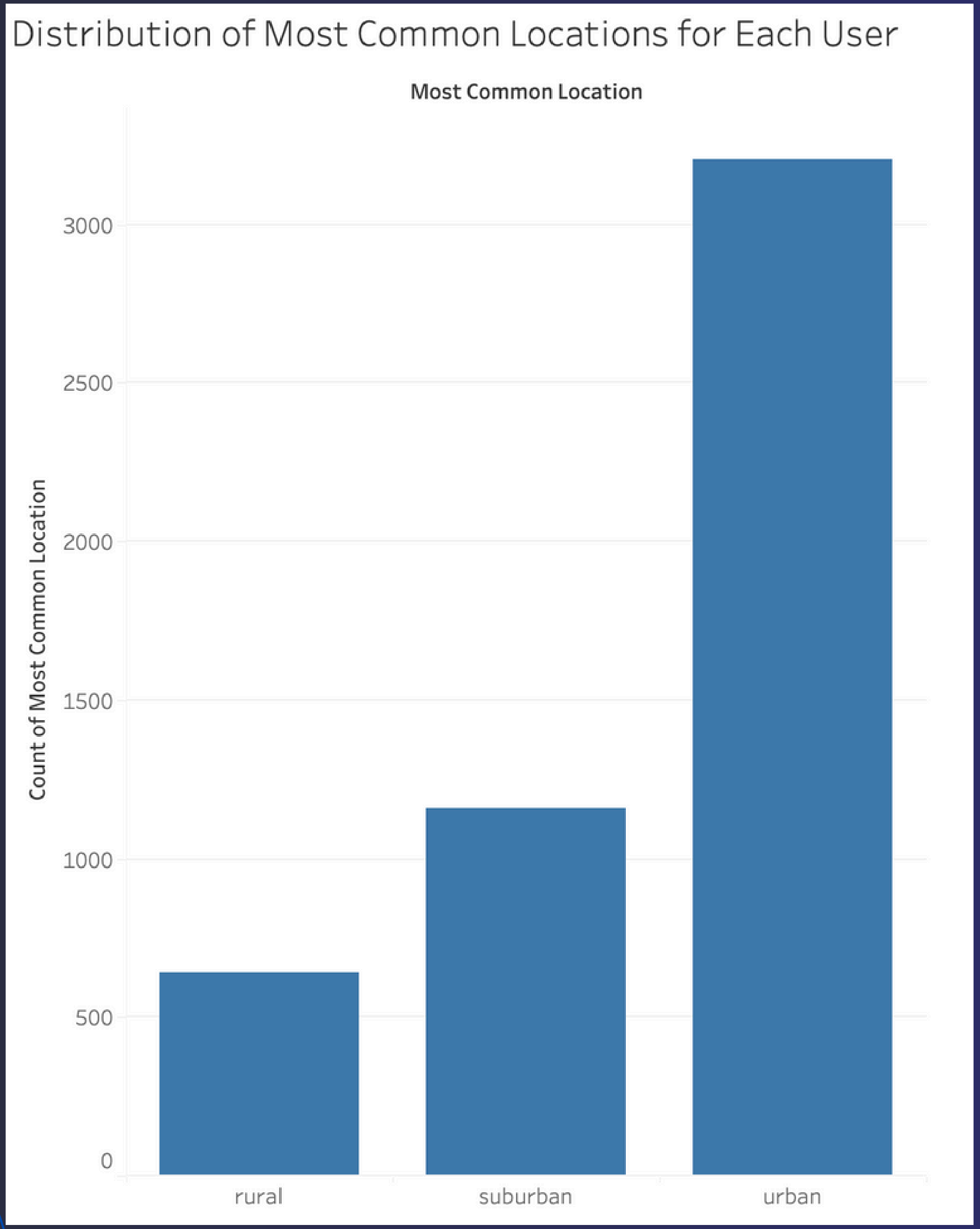


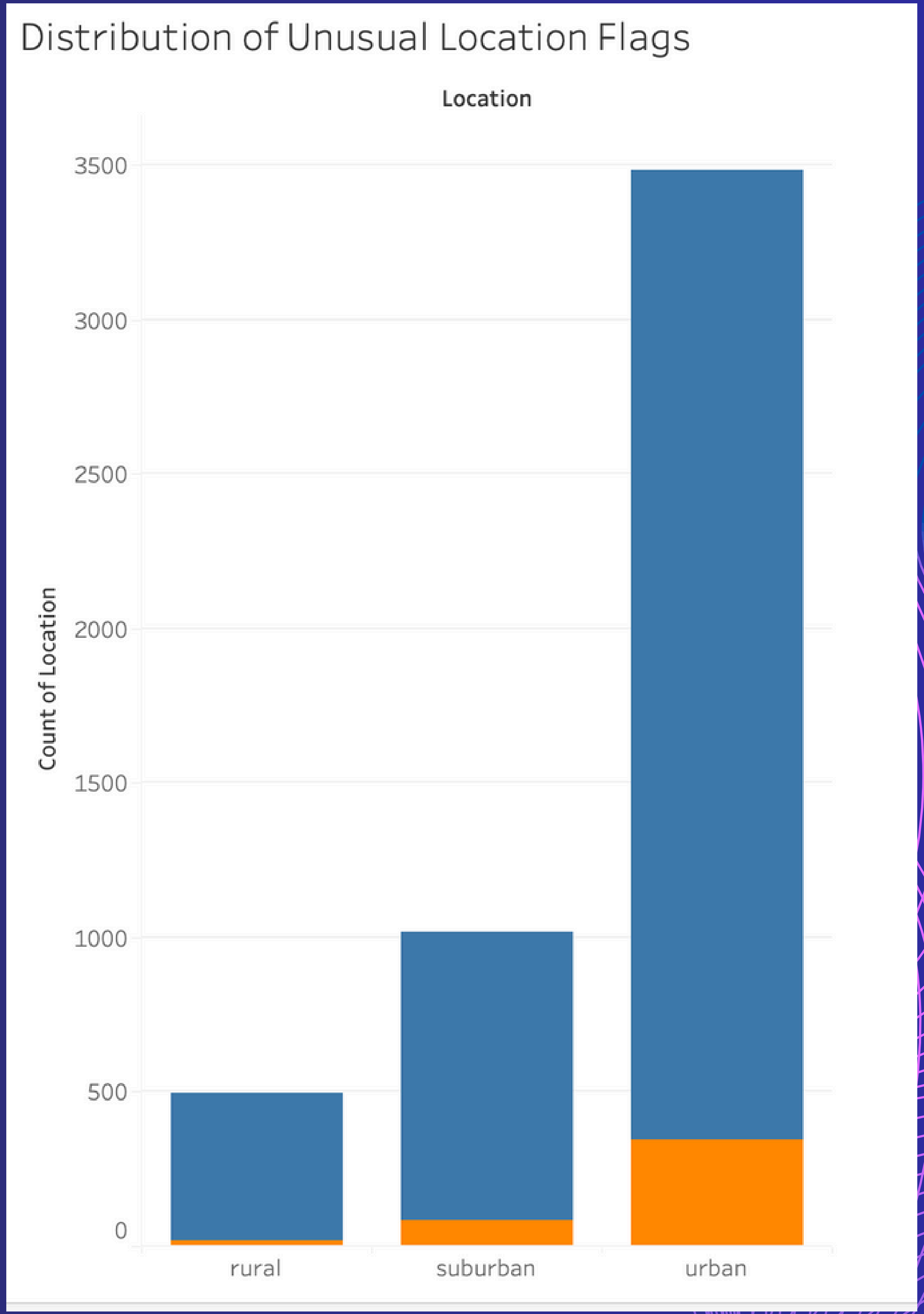


Indicator 3: Unusual Locations

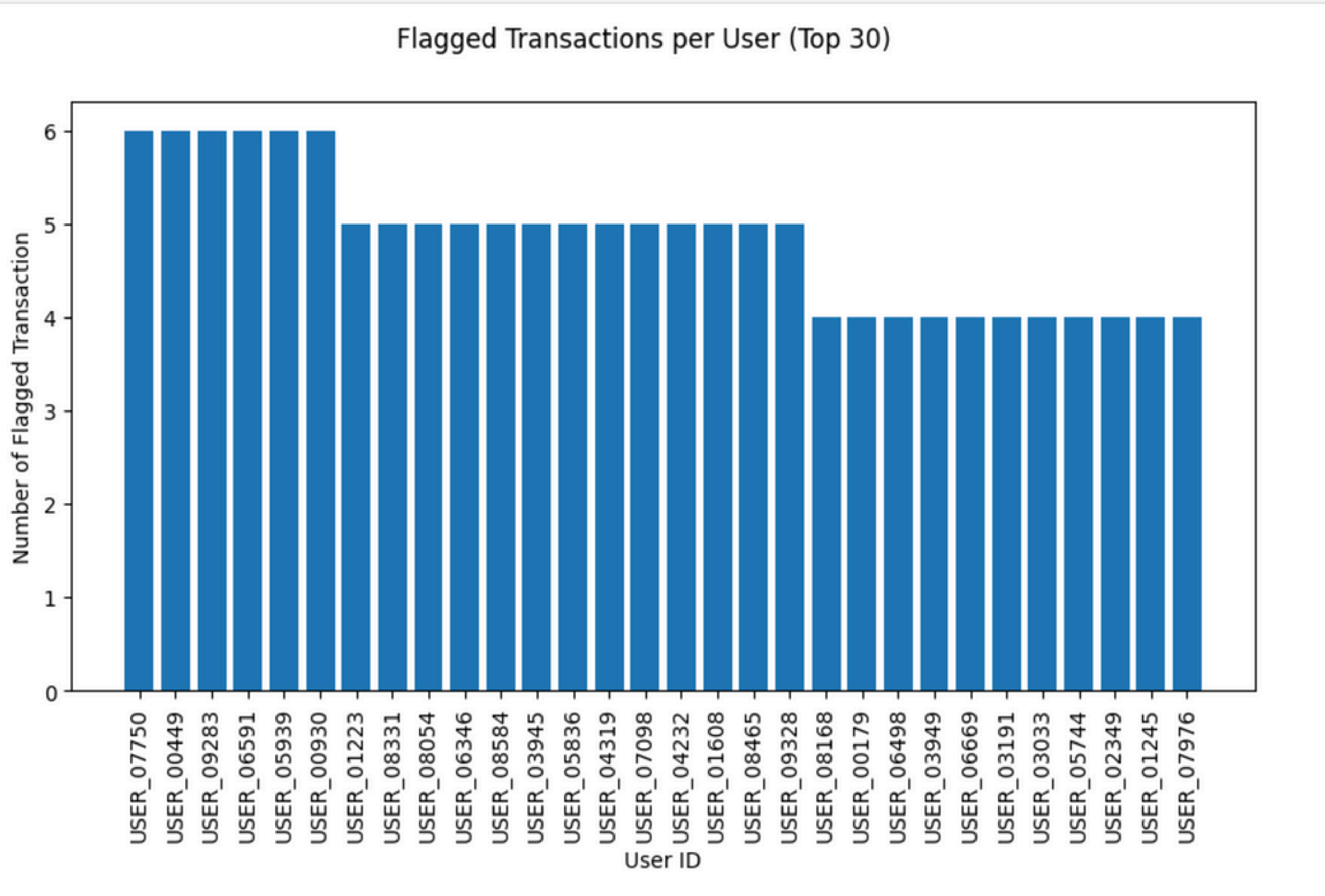
- Dataset provides three options for location data
  - Rural, Suburban, and Urban
- Determines the typical location for transactions for each user
- Flag transactions that occur outside usual locations
- While this dataset has simple locations, the same indicator can be extended to a dataset with more detailed location data

Indicator 3: Unusual Locations

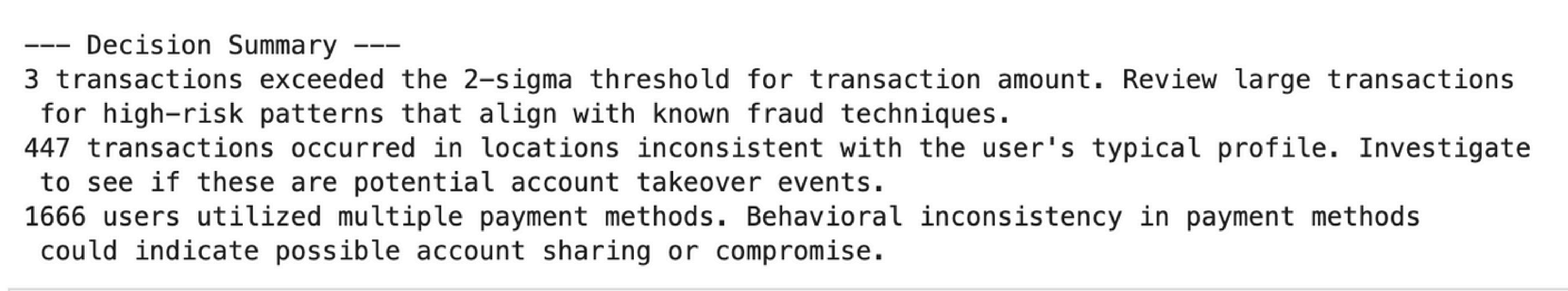




Insights from Indicators



- Evaluate and provide a summary based on flagged transactions
- Determine trends among different users
    - ○ Users with the highest number of flagged transactions



```
--- Decision Summary ---
3 transactions exceeded the 2-sigma threshold for transaction amount. Review large transactions
 for high-risk patterns that align with known fraud techniques.
447 transactions occurred in locations inconsistent with the user's typical profile. Investigate
 to see if these are potential account takeover events.
1666 users utilized multiple payment methods. Behavioral inconsistency in payment methods
 could indicate possible account sharing or compromise.
```

What are the Next Steps?

- Recommendations:
  - Implement automated fraud alerts based on key indicators.
  - Investigate **high-risk** patterns to refine detection systems.
- Next Steps:
  - Model training and validation.
  - Finalize report with actionable insights for deployment.

Thank you!