Fraud Analytics Summary Report

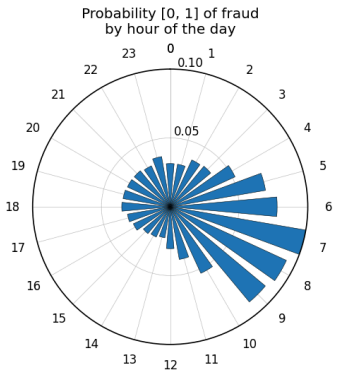
Juan Barbosa

1. Summary of Key Fraud Insights

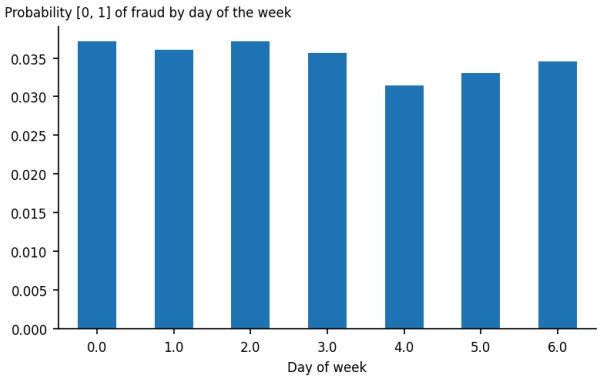
Based on the analysis of the transaction dataset, I have identified key fraud patterns and trends. The overall fraud rate in the dataset is approximately 3.5 %. A significant proportion of fraudulent transactions occur in specific categories such as **C1**, with 20 % of **C1** categories being five times riskier than the global average, accounting for 10 % of total fraud cases. This suggests that certain transactional behaviors or entities in these categories are exploited more frequently for fraudulent activity.

Key trends include:

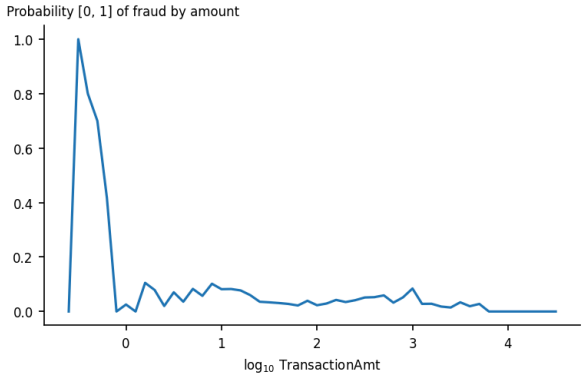
- **Peak Fraud Activity:** Fraudulent transactions tend to spike during early morning hours (4 AM - 10 AM), with 14% of fraud occurring in this window. A potential hypothesis is that fraudsters operate during low-traffic periods to evade detection.



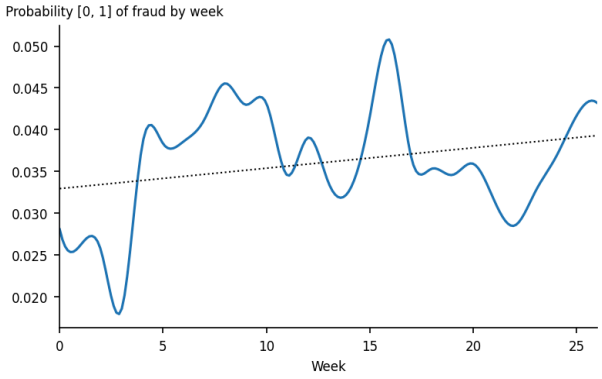
- **Day of the week:** Days 0 and 2 (likely Monday and Wednesday) show a 0.56 percentage point higher fraud rate than Day 4 (likely Friday), the least fraudulent. Days 4 to 6 (Friday to Sunday) exhibit an increasing fraud trend, possibly due to weekend spending patterns or reduced oversight.



- **Transaction Amount Patterns:** Transactions below $1 USD show an unusually high fraud risk. This is likely due to credential testing, where fraudsters use small amounts to verify if stolen card details are active. In contrast, transactions in the hundreds and tens of thousands exhibit lower risk, possibly because large transactions trigger manual verification, reducing fraud success.



- **Fraud rates over time:** The dataset spans six months, showing a general increase in fraud rates without a steady trend. No strong seasonal effects were detected, indicating fraud may be more opportunistic than cyclical.

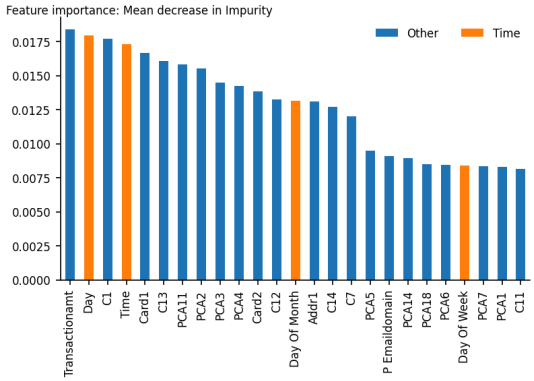


2. Fraud Risk Factors Identified

The model's feature importance analysis highlights the following key risk factors for fraudulent transactions:

1. **Transaction Amount:** Fraud risk is highest for transactions under $1 USD and moderate for small-range transactions ($1-$50 USD) and mid-range transactions ($500-1000$).
2. **Date:** All of the time features (day, time, day of week and day of month) are included within the top 25 features, that is the 10 % most relevant features.

3. **C1:** This property represents a count “such as how many addresses are found to be associated with the payment card, etc. The actual meaning is masked”**.** The category C1 has relevant predictive power as described in the trends.
4. **VXXX:** These columns are **“**engineered rich features, including ranking, counting, and other entity relations**”** ; the linear transformation of these columns proves to have relevance on identifying fraud transactions, as the first PCA column is within top 10 features.



4. Recommendations for Fraud Prevention

The model achieves a ROC AUC of 0.917, correctly identifying 42% of fraudulent transactions with minimal false positives (0.1% probability of being flagged with a legitimate transaction). However, further enhancements could improve detection rates and operational efficiency.

To improve fraud detection and reduce fraudulent transactions**:**

- **Customer-Specific Behavior Profiling:** By building features based on individual transaction history (e.g., average transaction amount, frequency), fraud detection can rely on behavioral deviations rather than fixed thresholds.
- **Novelty and Anomaly Detection:** Introducing unsupervised anomaly detection models alongside the current classifier can help flag previously unseen fraud tactics.
- **Real-Time Alerts & Monitoring:** The implemented Slack notification API (/api/v1/notify/slack) sends alerts for high-risk transactions. However, to improve fraud response, I recommend:
    - Automating Risk-Based Actions: Blocking transactions with extreme fraud probabilities (e.g., >95%) automatically.
    - Human Review: Flagging transactions with medium confidence (e.g., 70-90%) for manual investigation.
    - Tracking False Positives: Maintaining a feedback loop where incorrectly flagged transactions help refine model performance.