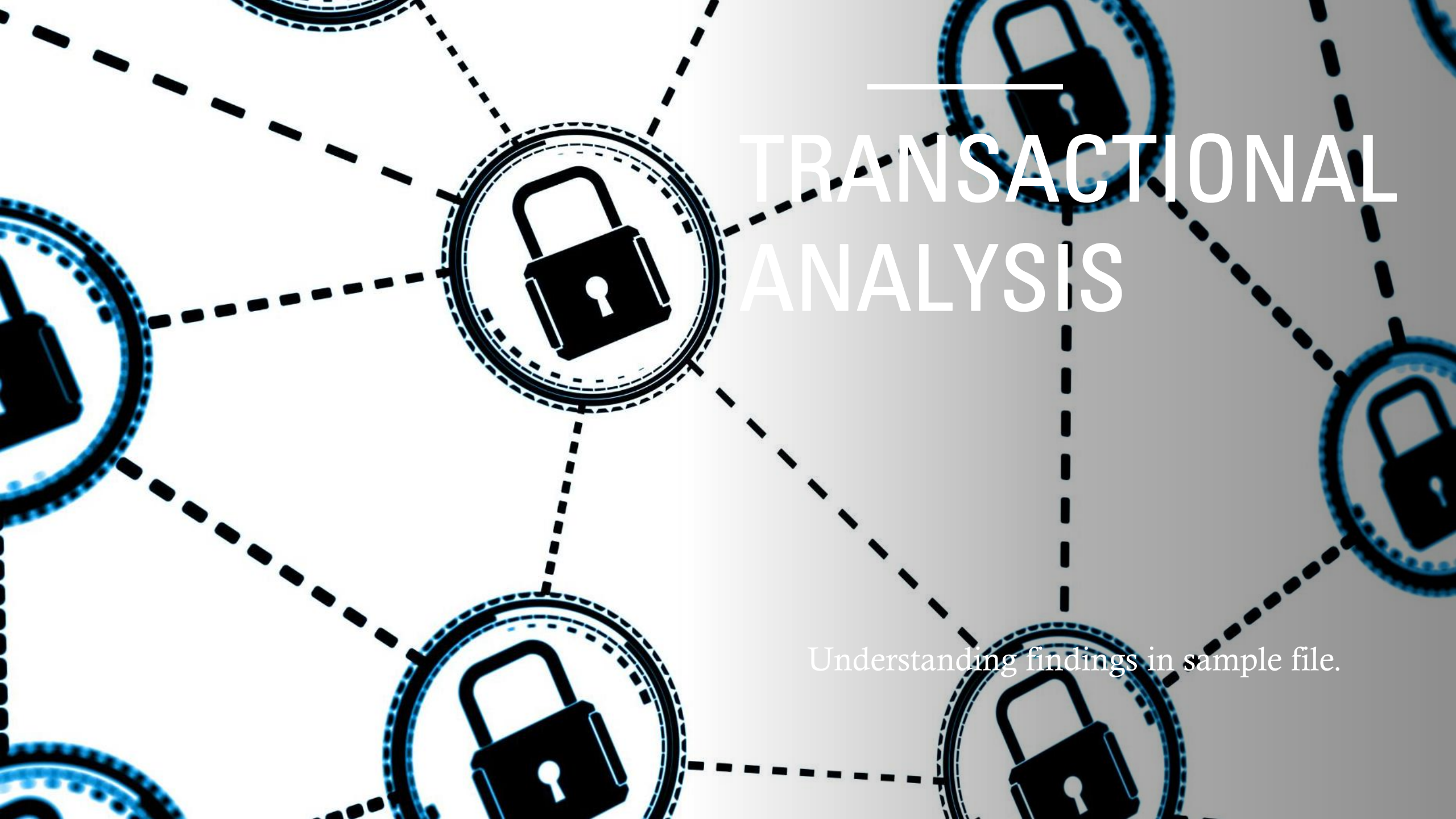


TRANSACTIONAL ANALYSIS

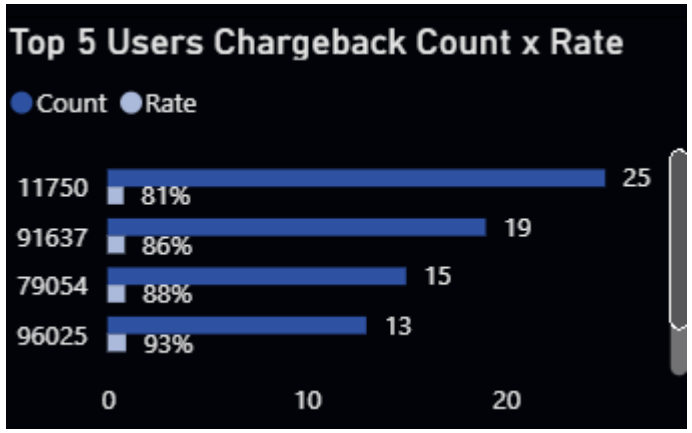
Understanding findings in sample file.

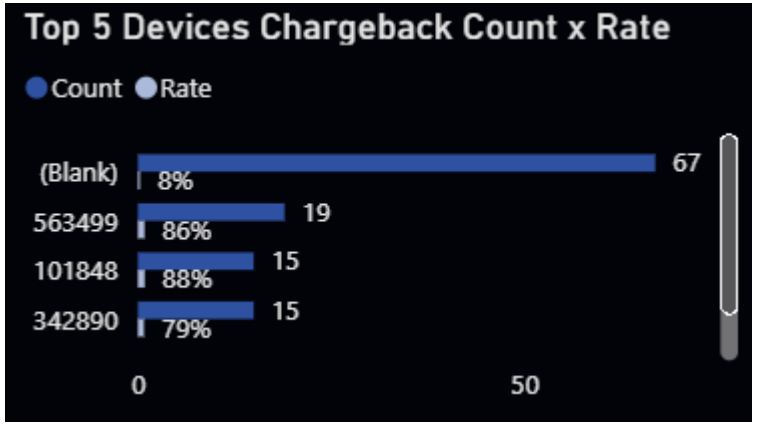
DISCUSSION TOPICS

- Data Analysis & Key Findings
- Additional Data to Enhance Fraud Detection
- Fraud & Chargeback Prevention Recommendations

DATA ANALYSIS & KEY FINDINGS

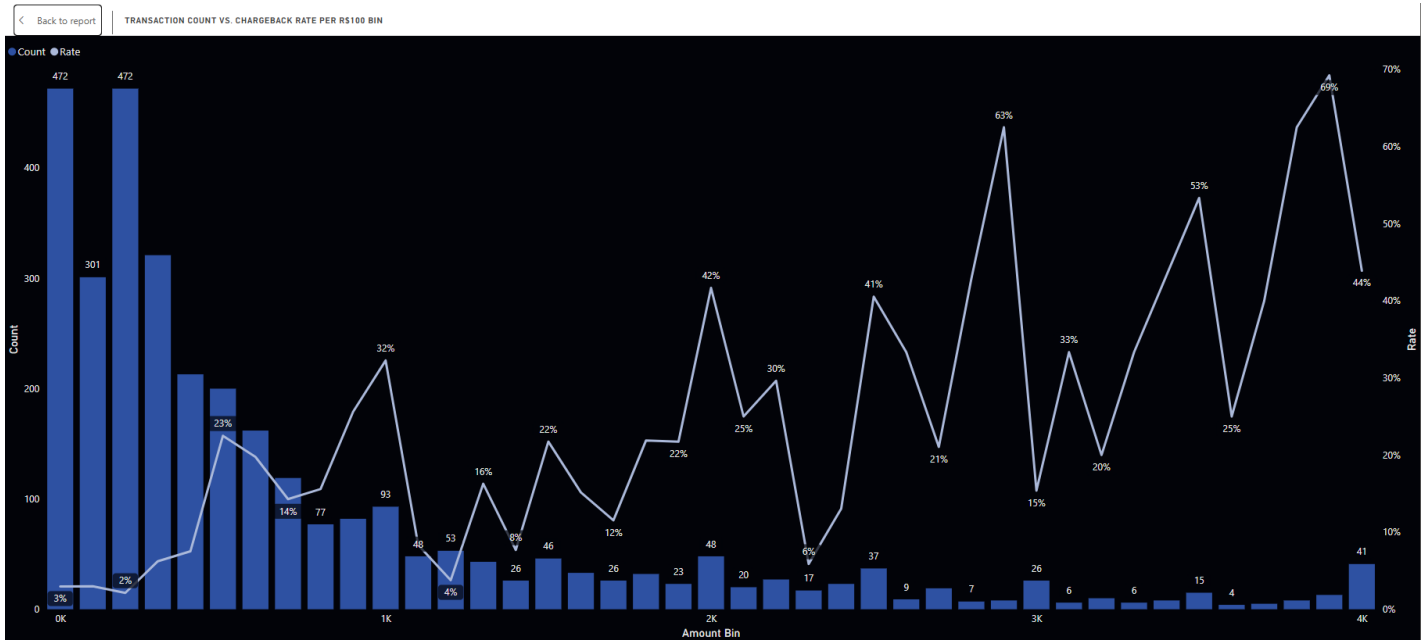
HIGH-RISK USERS & DEVICES





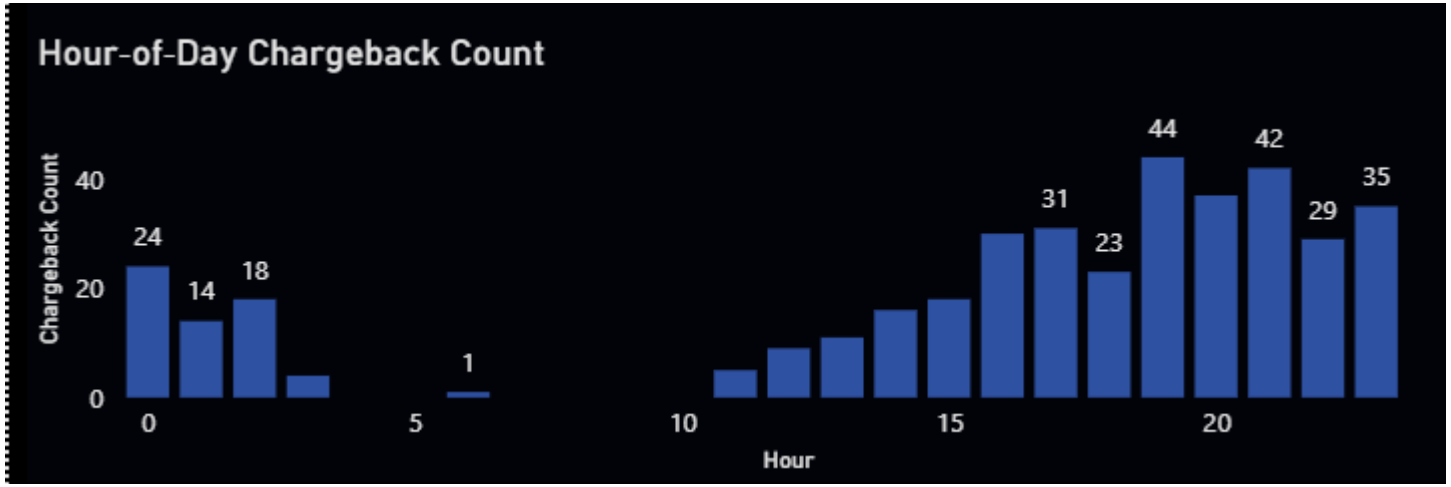
- The top 5 users account for disproportionately high chargeback rates (81%–93%), despite being a small fraction of total transactions.
- Similarly, a handful of devices show both elevated chargeback counts and rates (up to 93%).

AMOUNT BASED “TEST AND HIT” PATTERNS



- Chargeback frequency peaks in low-value bins (R$0–100 and R$100–200), then drops sharply, then briefly resurges at mid/high values, consistent with “test small amount → validate stolen card → commit larger fraud”.

TEMPORAL CLUSTERING



- Chargebacks cluster in off-peak hours, showing automated or scripted fraud tries when human review may be slowest.

ADDITIONAL DATA TO ENHANCE FRAUD DETECTION

FUTURE INTEGRATIONS

Device & Network Metadata

IP geolocation, VPN/proxy flags, browser fingerprint scores, and device fingerprinting.

Customer Profile & Historical Trends

Lifetime chargeback history, average order value per user, and account age.

Order Fulfillment Data

Shipping address velocity (same address used by multiple cards), carrier GPS stamps, and proof of delivery images.

External Fraud Feeds

BIN risk scores, global fraud deny lists, and peer network alerts from other merchants.

FRAUD & CHARGEBACK PREVENTION RECOMMENDATIONS

FRAUD PREVENTION RECOMMENDATIONS

Hybrid Rule-and-ML Engine

Enforce velocity/amount rules and time window restrictions.

Step-Up Authentication

Trigger 3D Secure or OTP verification for medium risk transactions (e.g., new device, high value purchase, or off hour order).

Manual Review & Rapid Response

Automatically route transactions above a specified risk threshold to a specialized team for the same day review.

Continuous Monitoring & Feedback Loop

Collect outcome data from disputes and chargeback representments to retrain the ML model and tune rule parameters, ensuring the system adapts to emerging fraud tactics.