CloudWalk Technical Case – Transactional Analysis

Data Analyst - Risk Analyst I

Daniel Sousa

1. Data Analysis & Key Findings

After examining the transactional dataset and Power BI dashboard (Total Transactions = 3199; Chargeback Rate = 12%; Unique Users = 2704; Unique Devices = 1997), I found suspicious behaviors:

- **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%).
  - **Conclusion:** Repeated disputes on the same user accounts or devices suggest credential-sharing, friendly fraud, or compromised credentials.
  - **Action:** Place these user_id/device_id pairs into a manual-review queue and enforce stricter verification (e.g., step-up authentication).
- **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".
  - **Action:** Implement dynamic amount-based velocity rules, declining or challenging multiple small transactions followed by large ones on the same device.
- **Temporal Clustering**
  - Chargebacks cluster in off-peak hours, showing automated or scripted fraud tries when human review may be slowest.
  - **Action:** Increase real-time monitoring and enforce lower risk thresholds during this time windows (e.g., require 3D Secure at 2 a.m.) (Stripe, 2025).

---

2. Additional Data to Enhance Fraud Detection

To uncover deeper fraud patterns, I recommend integrating:

- **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.

---

3. Fraud & Chargeback Prevention Recommendations
Building on these insights, I suggest:

1. **Hybrid Rule-and-ML Engine**
    - **Rule Module:** Enforce velocity/amount rules and time-window restrictions (e.g., max 2 small transactions/hour on same device) (Worldline, 2025).
    - **ML Module:** Train a supervised model on enriched features (device risk score, user history, amount bin) to output a dynamic risk score.
2. **Step-Up Authentication**
    - Trigger 3D Secure or OTP verification for medium-risk transactions (e.g., new device, high-value purchase, or off-hour order).
3. **Manual Review & Rapid Response**
    - Automatically route transactions above a specified risk threshold to a specialized team for the same day review (SEON Technologies Ltd., 2021).
4. **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.

References

SEON Technologies Ltd. (2021, August 30). *Chargeback Fraud Prevention Guide*. Retrieved from SEON: https://resources.cdn.seon.io/uploads/2021/08/Chargeback_Guide_08-30.pdf

Stripe. (2025, February 14). *3D Secure 101: What businesses need to know*. Retrieved from Stripe: https://stripe.com/resources/more/3d-secure-101

Worldline. (2025). *Fraud Detection Module*. Retrieved from Worldline: https://support.legacy.worldline-solutions.com/en/security/fraud-prevention/fraud-detection-module