Solution Proposal: Case Risk Analyst

Author: Marcelo Cruz

Email: marcelocrz.ds@gmail.com

Linkedin: https://www.linkedin.com/in/marcelocrz

Part 1: Practical Analysis

1.1. Analysis and Discovery of Suspicious Behaviors

Exploratory data analysis showed us that fraudulent behavior (transactions with has_cbk = True) is not randomly distributed. It is **concentrated in a few devices** and follows specific patterns.

Key Finding: Suspicious Device Detection

Further analysis revealed that a small number of devices are responsible for a large portion of the total loss.

- **Hypothesis:** Initial analysis showed that transactions with device_id had a higher fraud rate (13.7%) than transactions without device_id (8.1%).
- **Cause:** This does not happen because having a device_id is a problem, but rather because fraudsters were using the **same devices** to make several fraudulent purchases.
- **Impact:**
  - **Total number of chargebacks:** 391
  - **Suspicious devices** (defined as >3 transactions and >80% of the CBK fee): **17**
  - **Chargebacks caused by these 17 devices: 120**
- **Conclusion:**A group of just **17 devices** (less than 1% of total unique devices) was responsible for **30.69% of all chargeback losses** on the dataset.

Other Suspicious Behaviors Identified:

- **Speed Attack:** In the initial sample, we identified a user_id (81152) and device_id (486) making 3 fraudulent transactions in 20 minutes. This may indicate improper card use.
- **Absence of device_id in high-value transactions:** Transactions without device_id and with transaction_amounthigh levels have also been shown to be an indicator of risk.

1.2. Expanding the Analysis

The current analysis, focused on device_id, was able to explain ~31% of the fraud. To detect the remaining ~69%, which are likely more elaborate attacks (where the fraudster switches devices or uses other methods), it would be crucial to enrich the dataset with the following data:

- **Location data:**
    - **IP Address:** To identify transactions from distant locations, such as a user purchasing from São Paulo and 10 minutes later from Manaus, for example.
- **Card details:**
    - **Card BIN (first 6 digits):** Allows you to cross-reference the card issuing country with the country of the transaction (IP). A US card used in Brazil by a new user is suspicious.
- **User data:**
    - **Email Address:** Temporary or newly created emails are an indicator of risk.
    - **Account Age:** Accounts created within the last few minutes/hours have a higher risk of fraud.
- **Behavioral data:**
    - **Time Between Transactions:** Calculate the exact time (in seconds) since the last transaction of that user_id or device_id.

1.3. Recommendations and Preventive Measures

Based on the findings, the following measures could be implemented:

1. **Reactive:**
    - **Blocklist:** Add the 17 device_id identified high-risk emails to a blocklist. This isolated action would have prevented 120 chargebacks.
2. **Proactive:**
    - **Reputation system:** Create a "reputation" score for each device_id based on your transaction history and chargeback rate. New devices would have a neutral score that would be updated with each transaction.
    - **Speed rules:** Implement rules that limit the number of transactions allowed by a user_id, device_id or card_numberin short intervals of time (e.g. maximum of 3 transactions per card every 10 minutes).
    - **Two-factor authentication:** For medium risk transactions (e.g. high value and device_id absent), instead of refusing, request additional verification, such as authentication in the bank app.

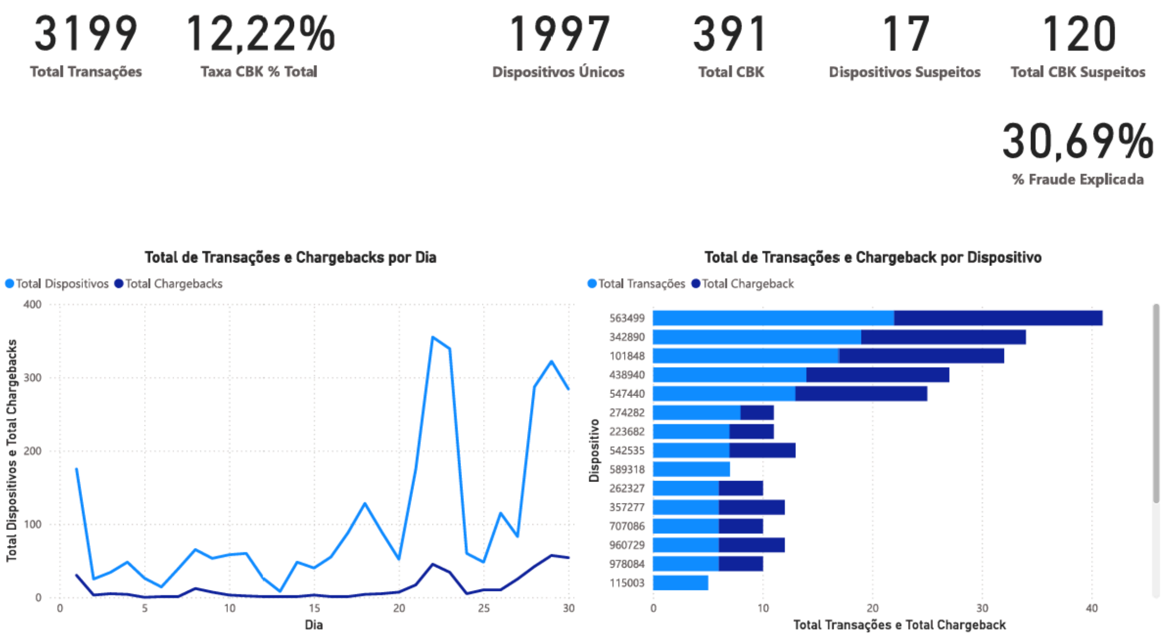
1.4. Anti-Fraud Solution

I propose a solution using rules and machine learning models.

1. **Part 1: Filter by rules**
    - Initial filter that blocks obvious fraud in milliseconds.
    - Verify the block list (device, user, IP, card BIN).
    - Applies speed rules.
2. **Part 2: Machine Learning Model**
    - Transactions that pass the rules filter are sent to a model that generates a **risk score (0-100)**.
    - **Features:** The model would be fed with features created from our analysis:

        - device_reputation (device historical CBK rate)
        - device_frequency (number of device transactions in the last 24 hours)
        - n_users_per_device_1d (number of unique users on that device in 1 day)
        - n_cards_per_device_1h (number of different cards in this device in 1 hour)
        - device_id_absent (0 or 1)
        - transaction_value
    - **Score-Based Actions:**
        - **Score 0-30 (Low Risk):** Automatically approves it.
        - **Score 31-70 (Medium Risk):** Sends for two-factor authentication.
        - **Score 71-100 (High Risk):** Automatically refuses.

1.5. Presentation of Results



3199
Total Transações

12,22%
Taxa CBK % Total

1997
Dispositivos Únicos

391
Total CBK

17
Dispositivos Suspeitos

120
Total CBK Suspeitos

30,69%
% Fraude Explicada

Total de Transações e Chargebacks por Dia
● Total Dispositivos ● Total Chargebacks
Total Dispositivos e Total Chargebacks
400
300
200
100
0
0
5
10
15
20
25
30
Dia
Total de Transações e Chargeback por Dispositivo
● Total Transações ● Total Chargeback
Dispositivo
563499
342890
101848
438940
547440
274282
223682
542535
589318
262327
357277
707086
960729
978084
115003
0
10
20
30
40
Total Transações e Total Chargeback

Part 2: Understanding the Industry

2.1. Payment Flow (Players and Flows)

- **Players:** Customer (Cardholder), Merchant, Payment Gateway, Acquirer, Brand and Issuing Bank.
- **Information flow (Authorization):** It's almost instantaneous (1-3 seconds).
    1. The customer enters data into the Merchant.
    2. Retailer sends data (via **Gateway**) to the **Purchaser**.

3. Purchaser sends to the**Flag**.
4. Flag sends it to the **Issuing Bank**.
5. **Issuing Bank** approve or deny and the answer makes its way back.

- **Financial flow (Settlement):** It's the flow of money, which is slower.
    1. **Issuing Bank** pay to **Purchaser** (via **Flag**).
    2. **Purchaser** deposit the amount into the account of**Shopkeeper**.

2.2. Acquirer vs. Sub-acquirer vs. Gateway

- **Payment gateway:** It is the **technology.** It works like the "card terminal" (machine) of the online world. It simply transmits transaction data securely between the merchant and the acquirer, but does not process the funds.
- **Purchaser:** It is the **financial institution**. It processes, settles the payment and assumes the financial risk.
- **By sub-acquirer:** And the **intermediary**. It uses an acquirer's infrastructure but simplifies the merchant's life. The sub-acquirer assumes the risk, facilitates integration, and passes the payment to the merchant.

2.3. Chargeback vs. Cancellation

- **Cancellation (or Refund/Reversal):** The customer contacts the store, requests a refund, and the store agrees and begins the refund process.
- **Chargeback:**The client doesn't recognize the purchase and goes directly to their bank (Issuer) to dispute the charge. The bank then forces the merchant to refund the money.

2.4. The Role of Anti-Fraud in the Acquirer

The anti-fraud system is what protects the **acquirer** and the **shopkeeper**. It is used to:

1. **Analyze risk in real time:** It sits between the gateway and acquiring processing, analyzing each transaction in milliseconds.before that it be sent to the flag.
2. **Minimize losses:**The main objective is to reduce **the number of chargebacks**, which represent a direct loss of money for the retailer and, in many cases, for the acquirer himself.
3. **Making decisions:**Based on the risk score, the anti-fraud system decides whether the transaction should be **approved, rejected** or sent to **authentication**.