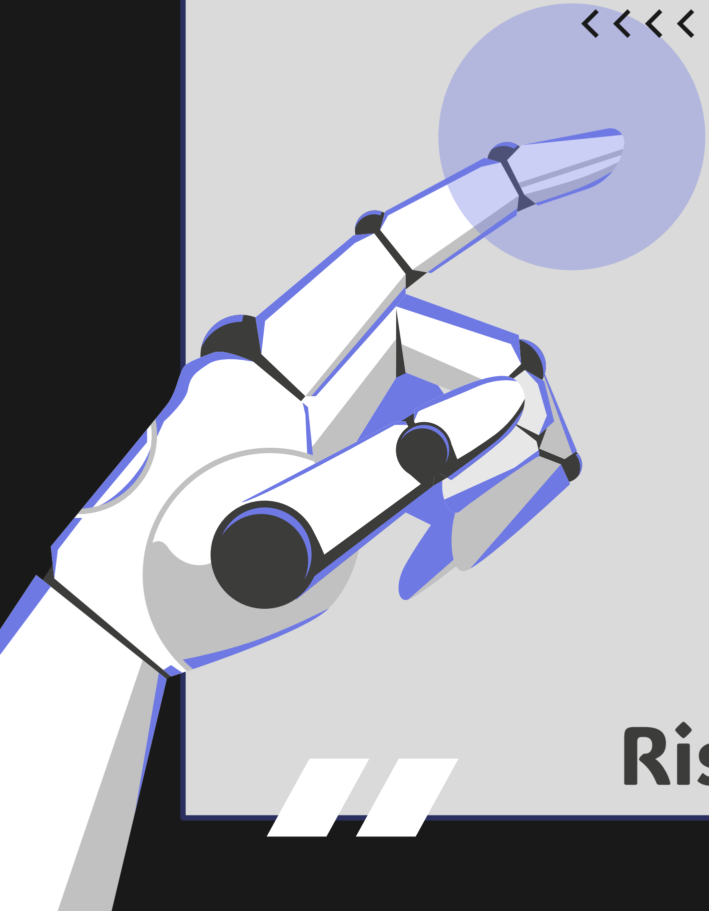


CASSIANO SOBIERAI

Case presentation

Risk Analyst I - CloudWalk

IN THIS PRESENTATION

THE PAYMENT INDUSTRY

CHARGEBACK SITUATION

GETTING THE HANDS DIRTY

THE PAYMENT INDUSTRY

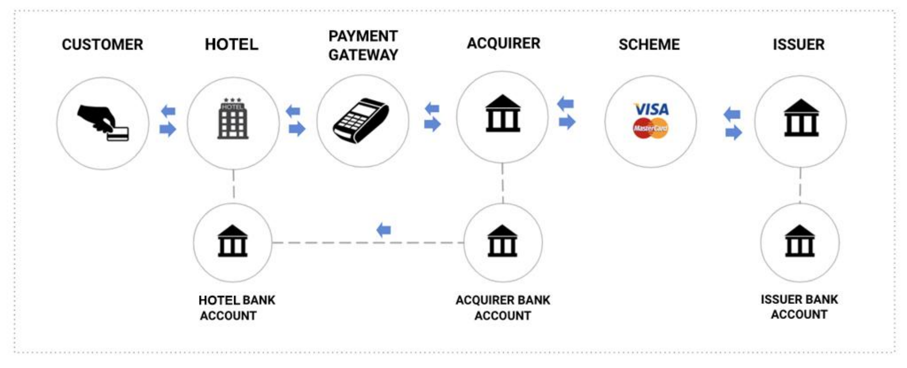
MONEY FLOW:

It begins when a cardholder (customer) makes a purchase from a merchant. The money is processed through the financial network, passing from the cardholder's bank (the issuer) to the acquirer bank account and is eventually transferred to the merchant's bank account.

CloudWalk works as a payment gateway and sub-acquier/acquirer

INFORMATION FLOW:

It begins when the customer uses their card to make a payment. The transaction data travels from the merchant to the payment gateway, then to the acquirer. From the acquirer, the information is sent to the card scheme and finally to the issuer. The issuer then authorizes/declines the transaction and the response is sent back along the same path to the merchant.



QUESTION 1

‹‹‹‹

DIFFERENCES

THE PAYMENT INDUSTRY

Payment Gateway: A technology that securely transmits payment data from the merchant to the acquirer.

Acquirer: A financial institution that processes payments for the merchant, has a direct relationship with the card scheme and handles the money flow.

Sub-acquirer: An intermediary that simplifies the process for the merchant, acting as a "merchant" to the acquirer.

THE FLOW CHANGES

With a Gateway: A technological layer is added to securely transmit data between the merchant and the acquirer. The money flow is unchanged.

With a Sub-acquirer: The sub-acquirer is positioned between the merchant and the acquirer, simplifying the integration for the merchant and altering both the data and money flow, as the sub-acquirer becomes the main point of contact.

QUESTION 2

THE PAYMENT INDUSTRY

THE CHARGEBACK CHALLENGE

A forced transaction reversal initiated by the cardholder through their bank. It is a consumer protection mechanism against unauthorized charges.

THE FRAUD CONNECTION

Chargebacks are a red flag for fraud. A high chargeback rate can indicate security vulnerabilities with merchants, leading to financial penalties and reputational damage.

QUESTION 3

THE PAYMENT INDUSTRY

ANTI FRAUD SYSTEM

Risk Analysis: Assess the risk of each transaction by considering factors like the buyer's history, purchase value, location and device type.

Prevention: Automatically block transactions that have a high probability of being fraudulent, protecting the merchant from financial losses and chargebacks.

Monitoring: Monitor customer and merchant behavior to detect unusual patterns that could indicate fraud.

Cost Reduction: Minimize costs associated with chargebacks and fraud losses, while also protecting the acquirer's and merchant's reputation.

CHARGEBACK SITUATION

SOLVING THE PROBLEM

1. Explain that the issuer denied the defense because the provided evidence was not considered sufficient to disprove the cardholder's claim of non-receipt.

2. Investigate if a new defense ("pre-arbitration") is possible and request stronger, more irrefutable evidence from the client, such as a signed proof of delivery.

3. Advise the client on the importance of obtaining robust proof of delivery for future transactions to prevent similar chargeback issues.

GETTING THE HANDS DIRTY

The dataset contains 3,199 card-not-present transactions across 8 columns.

Only *device_id* has missing values (830 nulls ≈ 26%).

The target variable *has_cbk* (chargeback due to fraud) is highly imbalanced.

- 12.2% fraudulent (True).
- 87.8% legitimate (False).

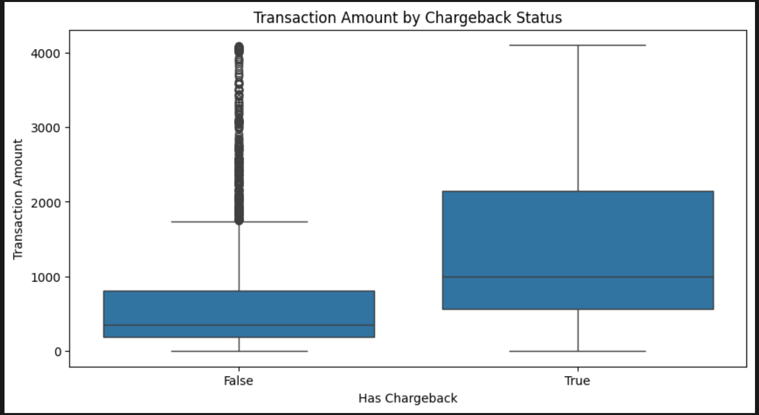
transaction_amount ranges from 1.22 to 4,097.21, with a mean of 767.81.

Period of one month.

DATA OVERVIEW

GETTING THE HANDS DIRTY

We can see that the most fraudulent transactions fall between the second and third quartiles (Q2 and Q3) of the transaction amount distribution.

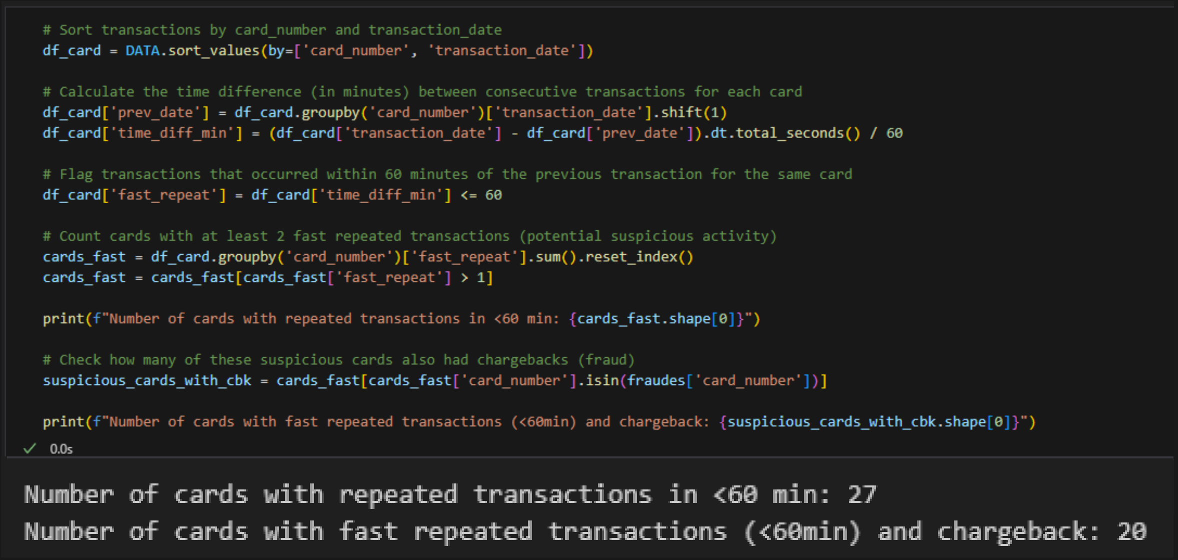


SUSPICIOUS BEHAVIORS

GETTING THE HANDS DIRTY

The more transactions made within a short period of time, the higher the likelihood of fraud.

When using *user_id*, the odds are even more significant.



```
# Sort transactions by card_number and transaction_date
df_card = DATA.sort_values(by=['card_number', 'transaction_date'])

# Calculate the time difference (in minutes) between consecutive transactions for each card
df_card['prev_date'] = df_card.groupby('card_number')['transaction_date'].shift(1)
df_card['time_diff_min'] = (df_card['transaction_date'] - df_card['prev_date']).dt.total_seconds() / 60

# Flag transactions that occurred within 60 minutes of the previous transaction for the same card
df_card['fast_repeat'] = df_card['time_diff_min'] <= 60

# Count cards with at least 2 fast repeated transactions (potential suspicious activity)
cards_fast = df_card.groupby('card_number')['fast_repeat'].sum().reset_index()
cards_fast = cards_fast[cards_fast['fast_repeat'] > 1]

print(f"Number of cards with repeated transactions in <60 min: {cards_fast.shape[0]}")

# Check how many of these suspicious cards also had chargebacks (fraud)
suspicious_cards_with_cbk = cards_fast[cards_fast['card_number'].isin(fraudes['card_number'])]

print(f"Number of cards with fast repeated transactions (<60min) and chargeback: {suspicious_cards_with_cbk.shape[0]}")
```

✓ 0.0s

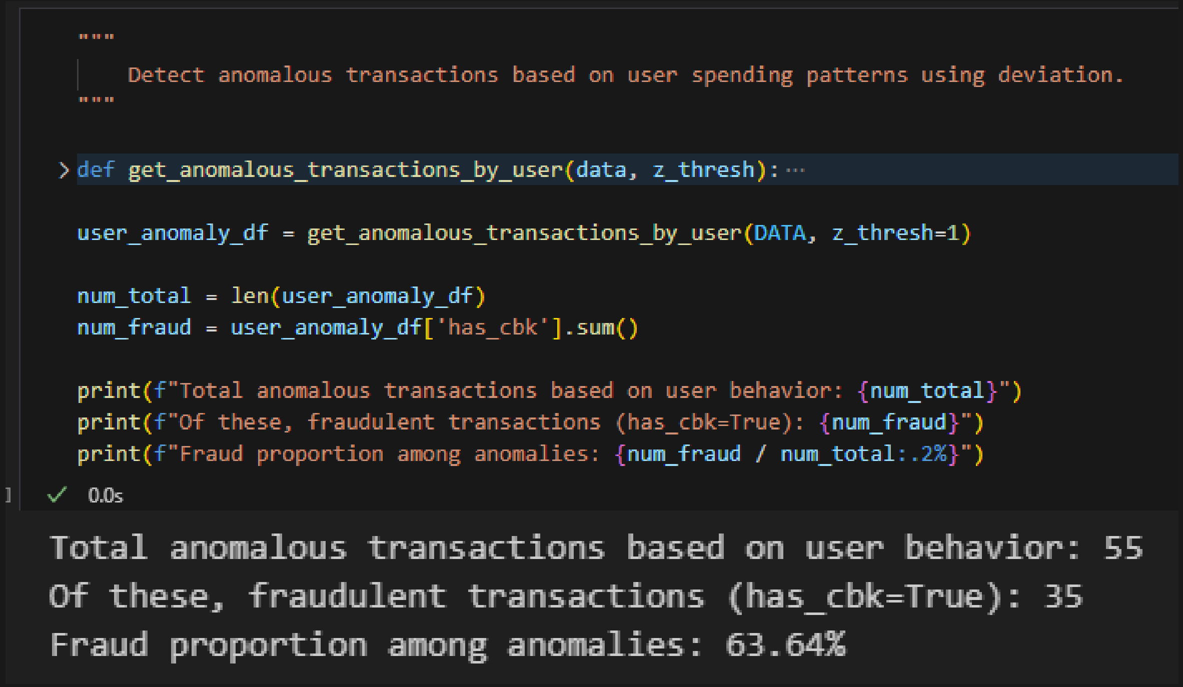
```
Number of cards with repeated transactions in <60 min: 27
Number of cards with fast repeated transactions (<60min) and chargeback: 20
```

SUSPICIOUS BEHAVIORS

GETTING THE HANDS DIRTY

The more a transaction amount deviates from a user's usual transaction, the higher the likelihood of it being fraudulent.

Method not worked for *merchant_id*.



```
"""
    Detect anomalous transactions based on user spending patterns using deviation.
"""

> def get_anomalous_transactions_by_user(data, z_thresh):···

user_anomaly_df = get_anomalous_transactions_by_user(DATA, z_thresh=1)

num_total = len(user_anomaly_df)
num_fraud = user_anomaly_df['has_cbk'].sum()

print(f"Total anomalous transactions based on user behavior: {num_total}")
print(f"Of these, fraudulent transactions (has_cbk=True): {num_fraud}")
print(f"Fraud proportion among anomalies: {num_fraud / num_total:.2%}")
```

```
Total anomalous transactions based on user behavior: 55
Of these, fraudulent transactions (has_cbk=True): 35
Fraud proportion among anomalies: 63.64%
```

SUSPICIOUS BEHAVIORS

GETTING THE HANDS DIRTY

/ / / / / / / / /

New implementation

Implement velocity rules to block or flag fast and repeated transactions.

Develop anomaly detection models for transaction amounts.

Prioritize the collection of *device_id* and flag transactions where it is missing.

Apply graph analysis to find suspicious connections between users, cards and merchants.

New data

Location Data: IP address, billing and shipping addresses.

User/Merchant Behavior: basics information, patterns and new cards.

Account Data: Chargeback history, account age and number of associated cards.

Graph Features: shared devices, cards or IPs to detect fraud networks.

ACTIONS

THANK YOU!

Any questions?
Get me in touch on cassianosobierai@outlook.com