Payment Analysis Test Case

Clesson Roberto da Silva Junior

- 2.1 – Understand the industry.

What is the acquirer market?

In every transaction, there are mainly three parties: the buyer, the seller, and what I'd like to call "the middleman." Which one has the best business? It's very hard to tell, but the middleman is virtually able to expand infinitely as long as they have the best platform or some kind of technological advantage.

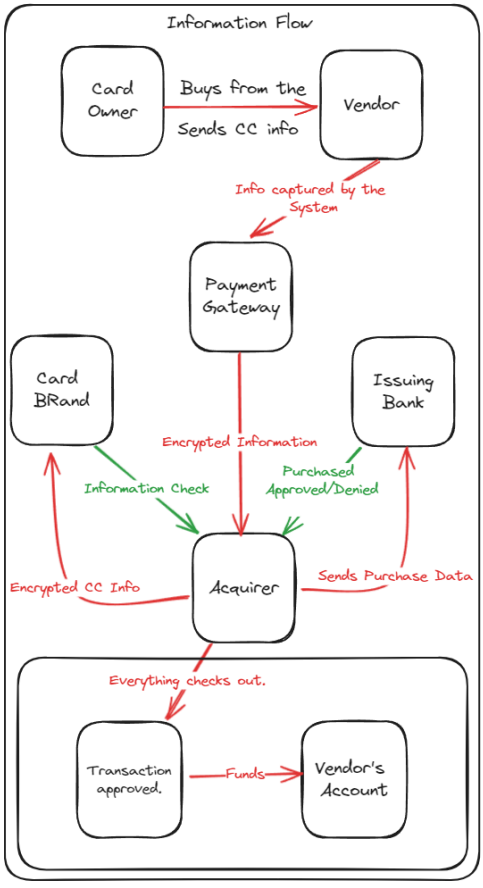
The “acquirer market” is born from this competition, being the best payment option. Although it seems like a very intuitive business, the challenges are significant, since you are the person that must guarantee a safe, fast, and efficient transaction. Considering a chargeback scenario, the focus should be on a credit card transaction.

- **1.** Explain the **money flow, information flow** in the acquirer market and **the role of the main players.**

Information Flow & Main Players

Prior to explaining the money flow, which is basically end-to-end, it’s important to create the structure formed by the main players that allow the information to flow.

Here’s a **quick diagram** to quickly visualize the whole system:



- **Card owner and Vendor:**
    - Usually, when a deal has taken place, a transaction initiates between the card owner and the vendor. The system/software chosen by the vendor will capture the data and send the details to the **payment gateway.**
- **Payment Gateway**
    - The payment gateway is responsible for capturing the information and sending it to **acquirers** (something very similar to a TCP handshake), and then waits for a confirmation that the data has been successfully sent. A good example would be a “cash register”, but in an electronic transaction.
- **Card Brand**
    - Responsible for creating the business rules for purchases using their specific credit cards. They create the rules which the **acquirer** must follow. It receives the information from the acquirer, validates the conditions, and sends the data to the issuing bank, which will then check the cardholder's available limit.
- **Issuing Bank**
    - It's the financial institution associated with the payment method. It receives the purchase data and, upon verification, authorizes or declines the sale.

- **Acquirer (This would be CloudWalk)**
    - The main payment processor, it receives the information from the Payment Gateway, and sends it to the **card brand, and the issuing bank.** Once all the info has been verified and the purchase is verified by all the parties, the acquirer must transfer the funds from the issuing bank to the vendor’s account.

Money flow

The funds essentially transfer from the cardholder's issuing bank to the vendor's account. However, the preceding verification steps in the information flow are necessary to approve the transaction, and some fees may also be deducted from the total value of the transaction, which is usually paid for by the vendor.

- **2.** Explain the difference between **acquirer, sub-acquirer and payment gateway** and how the flow explained in question 1 changes for these players.

  The **acquirer** is a big financial institution that processes credit/debit card transactions on behalf of a merchant, while the **sub-acquirer** stays between the merchant and the acquirer, it handles the initial processing of transactions, and then also sends it to an **acquirer**.

  Sub-acquires are usually used by small business that may not meet the requirements for a direct connection with a big acquirer, but their fees are a bit higher.

  The **payment gateway** securely transmits encrypted transaction information to the acquirer. In cases where a sub-acquirer exists, the payment gateway's functionality may be integrated within the sub-acquirer's services.

  The flow itself changes slightly: an authorization request is issued by the merchant, processing and validation is done by the intermediary **(sub-acquirer or payment gateway)**, it then communicates with card networks and issuing banks, authorization decision, and settlement of funds to the merchant's account.

- **3.** Explain what **chargebacks** are, how they differ from cancellations and what is their connection with fraud in the acquiring world.

A chargeback is intended to reclaim funds from transactions that are either fraudulent, unauthorized, or involve defective or undelivered products and services, ensuring the original payer is reimbursed.

A cancellation occurs when a transaction is voided or nullified before it is completed or fulfilled, thus avoiding any disputes. On the other hand, a chargeback takes place after a transaction has been finalized.

- 2.2 – Solve the problem.

The answer must perfectly balance what the data reveals, legal requirements, and client satisfaction. Therefore, I will thoroughly analyze the complete data again to ensure the right decision is made. The main data points will include shipping information and client stock receipts, which track the item destination flow.

Once this process is complete, there are two possible outcomes: either there was a mistake in the data, and the item has been delivered, or the item has not been delivered, in which case the client must take the loss, as the shipping risk is their responsibility.

After the analysis has been made, I'd respond to the client accordingly.

3. Get you hands dirty

- 3.1 Analyze the data provided and present your conclusions.
    - The full answer may be found in the Jupyter Notebook.
- 3.2 In addition to the spreadsheet data, what other data would you look at to try to find patterns of possible frauds?
    - In addition to the spreadsheet data, I would examine other data points to identify potential fraud patterns. These include IP/geolocation, cardholder's usual behavior (frequently bought items), average transactions per month, typical purchase times, etc. Essentially, creating a detailed profile for each customer. While this may be costly, it will significantly enhance the effectiveness of fraud detection.
- 3.3 Considering your conclusions, what could you do to prevent frauds and/or chargebacks?
    - While it may not be a conventional approach, the primary perpetrators of fraudulent activities are often quite adept at their craft, enabling them to execute large-scale fraud schemes effectively. While a well-trained machine learning model with adjusted weights can be highly effective in blocking the majority of fraudulent attempts, it may not be sufficient to thwart the most sophisticated fraudsters who can closely mimic the behavior of legitimate customers.
    - To address this challenge, further research is needed to identify the weak points in their emulation process and develop comprehensive solutions. In this regard, leveraging the expertise of ex-hackers or convicted 'pro carders' could prove valuable, as they possess the insight and perspective to anticipate and counter the tactics of their counterparts. Implementing such measures not only has the potential to significantly mitigate fraud but also instill greater confidence among stakeholders.