1. Introduction

If you get here, we already see you as a good fit for our company. Now, we propose a challenge similar to the ones you will face working with us. The challenge has three parts, created to help you build the knowledge needed to implement the technical assessment in the end.

- The first challenge will help you understand how the payments industry works.
- The second challenge is a real customer problem.
- The third challenge is similar to what you will be doing on a daily basis.

We expect you to grasp our role and the challenges within the financial industry, bringing innovative solutions to the table. Your evaluation will focus on logical reasoning, effective problem-solving, innovation, analytical mindset, customer centricity, and the performance of your solutions, rather than the aesthetics of your presentation.

2. Tasks

2.1. Understand the Industry

1. Explain briefly the money flow, the information flow and the role of the main players in the payment industry.
2. Explain the main differences between acquirer, sub-acquirer and payment gateway, and how the flow explained in the previous question changes for these players.
3. Explain what chargebacks are, how they differ from a cancellation and what is their connection with fraud in the acquiring world.
4. What is an anti-fraud and how an acquirer uses it.

2.2. Solve the problem

A client sends you an email asking for a chargeback status. You check the system, and see that we have received his defense documents and sent them to the issuer, but the issuer has not accepted our defense. They claim that the cardholder continued to affirm that she did not receive the product, and our documents were not sufficient to prove otherwise.

3. Get your hands dirty

Attached herein lies a spreadsheet with hypothetical transactional data. Imagine that you are trying to understand if there is any kind of suspicious behavior.

1. Analyze the data provided and present your conclusions. What suspicious behaviors did you find? What led you to this conclusion? What actions would you take?

2. In addition to the spreadsheet data, what other data would you consider to find patterns of possible fraudulent behavior?

3. Considering your conclusions, what would you further suggest in order to prevent frauds and/or chargebacks?

4. Create an anti-fraud solution.

5. Present your results and conclusions.

Some tips:
User_id: id of the cardholders;
Device_id: divide used by the cardholder;
Has_cbk: transaction received a fraud chargeback or not. All the transactions occurred in a card not present environment. You can use any programming language that you want.

Solution

2.1 Understand the Industry

2.1.1 Explain briefly the money flow, the information flow and the role of the main players in the payment industry.

The payment industry involves various flows and participants. We can break it down into three key categories: money flow, information flow, and the role of the main players. These components ensure the secure and efficient operation of electronic payments, credit card transactions, debit cards, electronic transfers, and digital wallets. Let's briefly explain each of these components.

1. Money Flow

The money flow refers to the path that money takes from the payer (consumer) to the recipient (merchant). This process involves the following steps:

1. **Consumer/Payer**: The consumer starts the transaction by purchasing a product or service, typically using a credit card, debit card, or digital wallet.
2. **Issuer Bank**: This is the bank that issues the credit or debit card to the consumer.
3. **Card Network (e.g., Visa, Mastercard)**: The card network acts as an intermediary between the issuer bank and the acquiring bank, facilitating the communication and transaction processing.
4. **Acquirer Bank**: This is the bank that processes the payment and credits the amount to the merchant.
5. **Merchant**: The merchant receives the net payment after fees are deducted by the acquirer, issuer bank, and card network.

Money Flow Summary:

1. The consumer makes the payment.
2. The issuer bank verifies the consumer’s balance or credit limit.
3. The transaction is routed by the card network to the acquirer.
4. The acquirer pays the merchant, deducting fees.

2. Information Flow

The information flow is the exchange of data between participants to authorize, validate, process, and settle a payment. The key steps include:

1. **Authorization**: When the consumer makes a purchase, the payment request is sent from the merchant to the acquirer, then to the card network, and finally to the issuer bank for approval.
2. **Authentication**: This step verifies the consumer's identity to prevent fraud (e.g., using passwords, biometrics).
3. **Settlement**: After authorization, the issuer bank sends the funds to the acquirer bank, ensuring the correct amount is transferred to the merchant.
4. **Reporting**: Transaction data is stored and used for reporting, verification, and resolving disputes.

Information Flow Summary:

1. The merchant sends the payment request to the acquirer.
2. The acquirer forwards the request to the card network, which sends it to the issuer.
3. The issuer approves or denies the payment.
4. Transaction data is stored for reporting and verification.

3. Role of Main Players

Key participants in the payment ecosystem play vital roles to ensure secure and reliable electronic transactions:

- **Consumer/Payer**: Purchases goods or services and interacts with the issuer and often a digital wallet.
- **Merchant**: Sells goods or services and receives payments via the acquirer.
- **Issuer Bank**: Provides credit or debit cards, authorizes payments, and manages the consumer's account.
- **Acquirer Bank**: Works with the merchant to process payments and ensure the merchant receives the funds.
- **Card Network (Visa, Mastercard, etc.)**: Facilitates communication between the issuer and acquirer and sets rules for transactions.
- **Payment Processors**: Third-party companies providing the technology to authorize and settle payments.
- **Payment Service Providers (PSPs)**: Platforms that allow merchants to accept various payment methods.
- **Payment Gateway**: Technology enabling merchants to accept online payments.

Main Players Summary:

- **Consumer**: Buys goods/services and pays.
- **Merchant**: Receives payment for goods/services.
- **Issuer Bank**: Authorizes and processes payments.
- **Acquirer Bank**: Receives and transfers payments to merchants.
- **Card Networks**: Enable communication between banks.
- **Processors and PSPs**: Provide tech support for transactions.

4. Fees Involved

Fees in a payment transaction include:

- **Issuer Fee**: Charged by the issuer bank to the acquirer.
- **Card Network Fee**: Charged by the card network for processing the transaction.
- **Acquirer Fee**: Charged by the acquirer to the merchant for processing the payment.

2.1.2 Explain the main differences between acquirer, sub-acquirer and payment gateway, and how the flow explained in the previous question changes for these players.

1. Acquirer (Acquiring Bank)
Definition: An acquirer is a financial institution (usually a bank) that works directly with merchants and processes payment transactions made with credit and debit cards.

Examples: Cielo, Rede, GetNet

Payment Flow:

- The acquirer connects directly to the card network, sends the authorization request to the issuing bank, and once the transaction is approved, the acquirer settles the amount with the merchant, charging a fee.
- The process mainly involves four parties: the merchant, the acquirer, the card network, and the issuing bank.

2. Sub-Acquirer

Definition: A sub-acquirer is an intermediary that provides payment processing services to merchants without requiring them to have direct contracts with an acquirer.

Examples: PagSeguro, Mercado Pago, Stone, InfinytePay

Payment Flow:

- The sub-acquirer collects transactions from several merchants and processes them through an acquirer. The payment flow for the merchant goes through the sub-acquirer, who works with the acquirer to process the transaction.
- The merchant doesn't deal directly with the acquirer or the card network; they only deal with the sub-acquirer.
- This adds an extra layer to the process: Merchant → Sub-Acquirer → Acquirer → Card Network → Issuing Bank.

3. Payment Gateway

Definition: A payment gateway is a software service that acts as a "channel" or "bridge" to send payment information from a merchant to an acquirer or sub-acquirer.

Note: A payment gateway doesn't process payments; it simply sends and receives data between the website and the financial institution.

Examples: Stripe, PayPal (when used as a gateway)

Payment Flow:

- The gateway facilitates communication between the merchant (or sub-acquirer) and the acquirer, ensuring the transaction data is transferred securely and quickly.
- The typical flow is: Merchant → Payment Gateway → Acquirer/Sub-Acquirer → Card Network → Issuing Bank.

How the Payment Flow Changes for Each Participant:

1. **For the Acquirer**:
    - Merchant → Acquirer → Card Network → Issuing Bank
    - The acquirer directly processes the transaction, connects to the card network, and the issuing bank. The merchant has a direct contract with the acquirer.
2. **For the Sub-Acquirer**:
    - Merchant → Sub-Acquirer → Acquirer → Card Network → Issuing Bank
    - The sub-acquirer handles the processing for multiple merchants through an acquirer. The merchant doesn't have a direct relationship with the acquirer or the card network.
3. **For the Payment Gateway**:
    - Merchant → Payment Gateway → Acquirer (or Sub-Acquirer) → Card Network → Issuing Bank
    - The payment gateway acts as a secure channel to send payment information, but the final processing is done by the acquirer or sub-acquirer.

Conclusion

The main difference between an acquirer, sub-acquirer, and payment gateway lies in their level of involvement with the merchant and how they connect to the card networks.

2.1.3 Explain what chargebacks are, how they differ from a cancellation and what is their connection with fraud in the acquiring world.

What is a Chargeback?

A chargeback is the process in which the value of a completed and processed transaction is refunded to the customer.

It occurs when a consumer questions or disputes a transaction, often claiming it was incorrect or fraudulent.

The refund process is carried out directly with the card network. Chargebacks can be requested for various reasons, such as:

- **Fraud**: The consumer claims they do not recognize the purchase, which may indicate unauthorized card use.
- **Service or product not delivered**: The consumer claims they did not receive the product or service they paid for.
- **Defective or non-compliant product**: The customer states that the product received does not match what was advertised or is faulty.
- **Billing error**: There was an incorrect charge (wrong amount, duplicate charge, etc.).

During a chargeback, the dispute may involve the consumer, the card issuer (issuing bank), the acquirer, and the merchant. The merchant has the opportunity to contest the chargeback by providing evidence that the transaction was legitimate.

What is a Cancellation?

A cancellation occurs before a transaction is completed and settled, meaning while the transaction is still pending.

If the merchant or consumer notices an error in the purchase or decides to cancel shortly after the transaction, a cancellation can be requested.

Since the transaction has not been finalized, the cancellation can be done easily, without the need for a formal dispute process, and the amount is adjusted immediately.

Differences Between Chargeback and Cancellation:

1. **Timing**:
    - **Chargeback**: Occurs after the transaction has been completed and processed by the issuing bank and acquirer.
    - **Cancellation**: Happens before the transaction is completed or right after authorization but before settlement.
2. **Complexity**:

- **Chargeback**: Involves a formal dispute process, which can include reviewing documents and analysis by multiple parties (issuer, acquirer, card network, and merchant).
- **Cancellation**: Is resolved directly between the merchant and the acquirer with less bureaucracy.

3. **Impact on the Merchant**:
   - **Chargeback**: The merchant may have the sale amount deducted from their account, and in cases of fraud or error, they may also face additional fees and risk damaging their reputation with the acquirer.
   - **Cancellation**: Is simpler and less harmful to the merchant since the transaction is not completed.

Conclusion

The main difference between chargebacks and cancellations lies in the timing of the transaction and how the refund is handled for the consumer.

While cancellations can be easily resolved before the transaction is settled, chargebacks involve disputes and may be triggered by fraud, such as unauthorized transactions or even friendly fraud.

Fraud prevention is essential to minimize chargebacks and protect merchants from significant financial losses.

2.1.4 What is an anti-fraud and how an acquirer uses it.

What is an Anti-Fraud System?

An anti-fraud system is a tool used to detect and prevent fraud in payment transactions. It analyzes information like card data, geolocation, purchase history, and customer behavior in real time to spot suspicious activities.

Acquirers (payment processors) use these systems to detect suspicious transactions, avoid financial losses, and reduce chargebacks (refunds) resulting from fraud.

How Acquirers Use Anti-Fraud Systems:

1. **Analyze risk in real time and block suspicious transactions.**

During the approval process, acquirers use anti-fraud systems to assess transaction risks in real time. When a customer makes a purchase, the transaction is checked against various metrics (e.g., location, purchase amount, buying behavior).
If unusual activity is detected, the transaction may be blocked, or additional verification may be required.

2. **Reduce chargebacks caused by fraud.**

By detecting and stopping fraud before the transaction is processed, acquirers significantly reduce the number of chargebacks related to fraudulent transactions. This protects merchants from financial losses and extra costs tied to refunds.

3. **Monitor transactions and alert merchants to possible fraud.**

The anti-fraud system continuously monitors a merchant's transactions and automatically notifies them when suspicious activities are detected. Merchants can choose to approve or block the transaction manually or allow the system to handle it automatically.

2.2 Solve the problem

A client sends you an email asking for a chargeback status. You check the system, and see that we have received his defense documents and sent them to the issuer, but the issuer has not accepted our defense. They claim that the cardholder continued to affirm that she did not receive the product, and our documents were not sufficient to prove otherwise.

You respond to our client informing that the issuer denied the defense, and the next day he emails you back, extremely angry and disappointed, claiming the product was delivered and that this chargeback is not right.

Considering that the chargeback reason is "Product/Service not provided", what would you do in this situation?

When a customer is unhappy and questions the issuer's decision regarding a chargeback, the best approach involves transparency, empathy, and a collaborative effort to resolve the issue.

Steps to Handle the Situation:

1. **Respond with Empathy and Professionalism**

Acknowledge the customer's frustration and show a willingness to help. This can diffuse the situation and demonstrate that the company takes the issue seriously. Be transparent about the next steps the company will take to try to reverse the decision.

2. **Review the Documentation**

Revisit the documents provided to the issuer. Check if any details were missed or omitted in the original defense. Useful documentation may include:

- **Proof of delivery with signature:** Detailed proof with the recipient's name, date, and signature.
- **Carrier communication:** Delivery details using GPS or tracking reports showing the product was delivered to the correct address.
- **Evidence of communication:** Emails or messages with the customer or carrier confirming delivery or scheduling.

3. **Communicate with the Issuer**

Reach out to the issuer, requesting a review of the case. Provide additional evidence of delivery and emphasize the merchant's willingness to cooperate for a fair resolution.

4. **Explore Alternatives**

If the issuer upholds the chargeback decision, consider other ways to mitigate the situation:

- **Offer a direct solution:** Depending on the company's policy, offering store credit or compensation can show goodwill and preserve the customer relationship.
- **Suggest the customer contacts their issuer:** Sometimes, it helps if the customer contacts their bank directly, especially if they have more evidence or information about the delivery.

5. **Keep the Customer Informed**

Regular updates, even without new information, show the company's commitment to resolving the issue. Keeping the customer in the loop helps reduce frustration.

Conclusion

Handling this situation requires patience and proactive measures. By responding empathetically, reviewing documentation, and exploring alternative solutions, the company demonstrates its dedication to customer satisfaction.

Even if the chargeback isn't reversed, offering alternatives and a willingness to resolve the issue can help maintain a positive relationship with the customer.