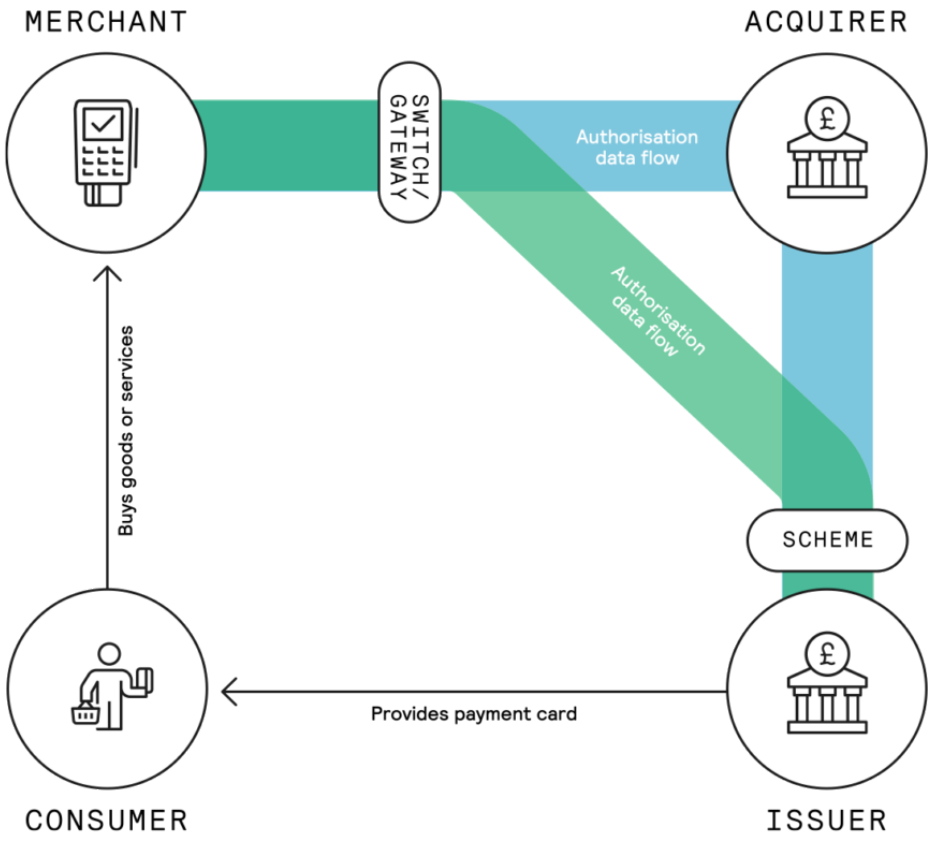
Task 2:

1. Understand the Industry

1. Explain the money flow, the information flow, and the role of the main players in
the payment industry.
2. Explain the difference 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.

Question 2.1.1 and 2.1.2:



1. **Consumer**: This is the individual making a purchase. They initiate the payment process by presenting their card details (or other payment information) to the merchant for the goods or services they want to purchase.
2. **Merchant**: This is the business selling goods or services. They take the payment information from the consumer and submit it through their payment gateway.
3. **Payment Gateway**: This is a service provided to the merchant to authorize credit card or direct payments processing for e-businesses and online retailers. It's

essentially the digital equivalent of a physical point-of-sale terminal located in most retail outlets. The payment gateway encrypts sensitive credit card details to ensure that information is passed securely from the consumer to the merchant, then from the merchant to the acquirer.

4. **Acquirer (Merchant Bank)**: This is a bank or financial institution that processes credit or debit card payments on behalf of a merchant. The acquirer receives the transaction details from the payment gateway, then they forward these details to the relevant card scheme.
5. **Sub-Acquirer**: This is a business that has a relationship with an acquirer to extend acquiring services to merchants. Sub-acquirers allow smaller businesses to accept card payments without needing to establish a direct relationship with an acquiring bank. The sub-acquirer forwards transaction details to the acquirer, who then sends these to the card scheme.
6. **Card Scheme (Card Network)**: These are institutions like Visa, MasterCard, or American Express. They act as the intermediary between the acquirer and the issuer. They pass on the transaction details from the acquirer to the card issuer.
7. **Issuer (Cardholder's Bank)**: This is the financial institution that issued the card being used for the transaction to the consumer. The issuer checks the transaction details and the consumer's account. If there are sufficient funds (or credit) and no security issues, they authorize the transaction. The issuer then sends the authorization back through the card scheme, to the acquirer, and then back to the merchant via the payment gateway.
8. **Settlement**: After authorization, the transaction isn't complete yet. The issuer will transfer the funds for the transaction to the acquirer, who then deposits the funds into the merchant's account. This process can take a couple of days.

Question 2.1.3

Chargebacks:

A chargeback is a transaction reversal meant to serve as a form of consumer protection from fraudulent activity committed by both merchants and individuals. A chargeback is initiated by the cardholder's bank (the issuer) and occurs when a customer disputes a charge on their card with their issuing bank rather than requesting a refund directly from the merchant.

Here's how it works:

1. The cardholder files a dispute with their bank, claiming a problem with a transaction, such as not receiving the goods or services they paid for, receiving faulty products, or being a victim of fraud or identity theft.
2. The issuing bank reviews the claim. If they deem it valid, they will withdraw the funds from the merchant's account and return them to the cardholder. The issuing bank also levies a chargeback fee on the merchant.
3. The merchant can dispute the chargeback if they believe the transaction was legitimate. If they provide sufficient evidence, the issuing bank may re-deposit the funds to the merchant's account. If not, the chargeback stands, and the consumer keeps the refunded amount.

Chargebacks vs. Cancellations:

While both chargebacks and cancellations can result in the consumer getting their money back, they're not the same:

- A cancellation is a straightforward process initiated by the customer or the merchant where the order is canceled, and the merchant processes a refund. This typically happens when a customer changes their mind about a purchase, and the merchant agrees to cancel the transaction and refund the money. The process is direct and doesn't involve banks or card networks.
- A chargeback, as described above, is a more complicated process initiated by the cardholder and involves multiple parties including the merchant, the issuing bank, and potentially the acquiring bank and card network. It's usually used when a customer and merchant can't agree on a refund, or when the customer doesn't recognize a transaction on their statement.

Connection with Fraud in the Acquiring World:

Chargebacks are closely related to fraud in the acquiring world:

1. Fraudulent Transactions: This happens when a fraudster uses a stolen card or card details to make purchases. The actual cardholder might not be aware of the transaction and files a chargeback when they see the unauthorized charge on their statement.
2. Friendly Fraud (or Chargeback Fraud): This occurs when a cardholder knowingly attempts to reverse a legitimate charge. They might claim that they never received an item, didn't authorize a purchase, or were unsatisfied with a product or service, even if none of that is true.

3. Merchant Fraud: A merchant could also commit fraud by charging a customer without delivering the goods or services, or by not accurately describing the goods or services. In these cases, a chargeback can protect the customer.

Chargebacks can be costly for merchants, not only because of the lost revenue and product but also due to fees and the administrative costs associated with managing chargeback disputes. If a merchant gets too many chargebacks, the acquiring bank might terminate their account, which could make it difficult for the merchant to get another acquirer to accept them.

Task 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?*

In this situation, it's important to reassure the client that you **understand** their frustration and you're there to help. Here's a step-by-step course of action:

1. **Acknowledge the Client's Frustration**: First, respond promptly to the client's email, acknowledge their frustration, and reassure them that you're there to help.
2. **Review the Case**: Go through the case again. Make sure that all the information is correct and that you understand the situation fully. This includes the client's defense documents, the delivery proof, and the issuer's response.
3. **Gather More Evidence**: If the issuer is stating that the evidence provided was not sufficient, ask the client if they can provide additional proof of delivery. This might be

a signed delivery receipt, tracking information, email confirmation of delivery from the courier, or even a signed statement from the delivery company confirming that the product was delivered to the correct address.

4. **Re-present the Chargeback**: Once you have gathered all additional evidence, you can re-present the chargeback to the issuer, including all the new evidence. The issuer will then review the new evidence and make a decision.
5. **Communicate**: Throughout this process, keep the client informed. Let them know that you're working on their case, that you've requested additional evidence, and that you've re-presented the chargeback to the issuer.
6. **Follow Up**: After re-presenting the chargeback, follow up regularly with the issuer to check on the status of the chargeback. Once you have an update, inform the client promptly.

Remember, **communication is key**. Ensure the client knows they are not alone in this and that you are doing everything in your power to resolve the issue in their favor. However, also inform them that the final decision rests with the issuer, and while you can present the strongest case possible, the outcome is not entirely within your control.

Task 3 - Get your hands dirty

Attached there's 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.*
2. *In addition to the spreadsheet data, what other data would you look at to try to find patterns of possible frauds?*
3. *Considering your conclusions, what could you do to prevent frauds and/or chargebacks?*
4. *How would you monitor identified patterns?*

To identify potential fraudulent behavior, you would typically use a combination of spreadsheet data analysis, additional contextual data, and machine learning algorithms.

In this project, I created a program that analyzes all the transactions from that spreadsheet and returns a JSON with all the ones that should be considered suspect and the reason for that.

Here's a little bit about the other questions from this task:

1. Spreadsheet Data Analysis: You'd first look for patterns in the spreadsheet data that could indicate suspicious behavior. For example:

- **Multiple Transactions in a Short Time**: A user making several high-value transactions in a short time span might be suspicious.
- **Repeated Chargebacks**: If a user has a history of chargebacks, it could be a sign of "friendly fraud."
- **Multiple Cards or Terminals**: If a user is using multiple cards or making transactions from multiple terminals in a short period, it could be a sign of stolen card information.
- **Odd Transaction Values**: Unusually high or low transaction values could also indicate fraud.

2. Additional Data: In addition to the spreadsheet data, you might also look at:

- **Location Data**: If a card is being used in multiple locations in a short time, it could be a sign of fraud.
- **IP Addresses**: Multiple transactions from different IP addresses could indicate fraudulent behavior.
- **Device Information**: If a user is constantly changing devices, it could be suspicious.

3. Preventing Fraud and Chargebacks: Based on your findings, you could implement several measures to prevent fraud and chargebacks:

- **Secure Authentication**: Implement multi-factor authentication to verify the user's identity during transactions.
- **Real-Time Alerts**: Set up real-time alerts for suspicious activity like multiple transactions in a short time, high-value transactions, or transactions from multiple locations.
- **User Education**: Educate your users about secure practices and how to spot and report potential fraud.
- **Strict Monitoring of High-Risk Users**: If a user has a history of chargebacks or suspicious behavior, monitor their activity closely.

4. Monitoring Identified Patterns: Once you've identified potential patterns of fraud, you need to continuously monitor them:

- **Machine Learning Algorithms**: Use machine learning algorithms to detect and alert about suspicious behavior. These algorithms can learn from past patterns and improve their detection capabilities over time.
- **Regular Data Analysis**: Regularly analyze transaction data to identify new patterns and trends.
- **Feedback Loop**: If a potential fraud is identified and confirmed, use this information to improve your detection algorithms and processes. If a potential fraud turns out to be a false positive, use this information to reduce false positives in the future.

Remember, fraud detection is a continuous process and needs to be constantly updated and improved as fraudsters change their tactics.

Task 4 - Solve the problem:

For this task, we will use our program. Please consider reading the Readme inside this project for further instructions on how to operate it.

It has 3 main functions:

1. Analyze an individual transaction;
2. Analyze all transactions;
3. Simulate and analyze, real-time, if a transaction can be approved or not.

When running the program, a prompt will appear asking what option you will take. If you select option 1, you should provide a transaction ID - from the spreadsheet .

For option 2, a JSON file will be created with all the denied transactions IDs and reasons for each one of them.

Option 3 will ask you for User ID and transaction value. The output is the approval or denied status and the reason for that.

First, I tried coding something using OpenAI but, even after several hours, I couldn't load the entire CSV to OpenAI read. Later I discovered that, basically, all Large Language Models are not that good at reading large files with data. I tried to split it, but everytime I asked how many transactions did you analyze, the answer was around 25 transactions.

Anyway, I scrubbed it and started from the beginning. It's a basic Python file that relies on some tasks and rules:

1. First, we analyze all the data and save in a different file all user IDs that had at least one chargeback. We also save the timestamp for the first chargeback from each user.
2. After that, we defined 3 main rules:
    a. Too many transactions in a row;
    b. Value above the average from that user;
    c. If the user had a chargeback anytime before the transaction.
3. All the rules above can be easily changed, since I defined some multipliers and hard-coded numbers like: how many transactions I'd allow in a row, percentage above average value permitted, etc…
4. Even when analyzing one or all transactions, the answer should be like: Transaction ID and approved or Transaction ID, rejected and reason (too many, high value, chargeback)

Final considerations

This project is basic and shows a little bit of how we can analyze transactions. There's some room for improvement and corrections, but the thing is, I'm ready to work with an already developed tool to use it in CW's favor. Despite not having the experience, I bring the thirst for knowledge and eagerness to learn. You'll have an avid team member among the squad!