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

Money Flow Translation:
Initiation: The process begins with the **payer** (who can be an individual or a company) initiating a transaction. This can be done through various channels, such as debit cards, credit cards, bank transfers, digital platforms, etc.
Authorization: The payment request is sent to the **authorizer**, which verifies if there is sufficient balance, if the account is active, and if the transaction is within the predefined limits.
Processing: After authorization, the transaction is processed by a **payment network**, which ensures communication between the authorizer, the payer's bank, and the recipient's bank.
Settlement: The money is then transferred from the payer's account to the **recipient's** account. This process may take a few days, depending on the payment method used.

Information Flow:
Transaction Data: For each transaction, information such as amount, date, time, location, and payment type is collected and stored.
Data Sharing: This data is shared among the various players in the industry, such as banks, payment networks, and acquirers, to ensure the security and traceability of transactions.
Data Analysis: The collected information is analyzed to identify purchasing patterns, combat fraud, and offer personalized products and services to customers.

Key Players:
Payer: The individual or company making the payment.
Payee: The individual or company receiving the payment.
Issuing Bank: The financial institution that issues the debit or credit card used by the payer.
Receiving Bank: The financial institution that receives the transaction amount for the payee.
Authorizer: The entity responsible for verifying that the transaction is authorized.
Payment Network: The infrastructure that connects the various players in the industry and ensures communication between them.
Acquirer: The company that allows merchants to accept card payments.

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.

Acquirer Translation:

Function: A company accredited by card brands (Visa, Mastercard, etc.) to process debit and credit card payments in physical and online stores.
Payment Flow:
Customer makes a card payment at a store or online platform.
Store/platform sends transaction data to the acquirer.
Acquirer verifies card validity, available balance, and authorizes the transaction.
Acquirer captures the sale amount and deposits it into the merchant's account (within a predetermined period).
Acquirer forwards transaction information to the card brand.
Card brand settles the amount with the card issuing bank.

Sub-acquirer:

Function: A company that is not directly accredited by the card brands, but rather by a principal acquirer. It offers payment services to other businesses, such as marketplaces, fintechs, and SaaS.
Payment Flow:
Customer makes a card payment on the sub-acquirer's platform.
Sub-acquirer sends transaction data to the principal acquirer.
The flow follows the same as the principal acquirer (items 3 to 6).
Principal acquirer forwards a portion of the transaction fee to the sub-acquirer.
Sub-acquirer deposits the sale amount into the merchant's account (within a predetermined period).

Payment Gateway:

Function: A platform that connects online stores and acquirers, facilitating the processing of payments in e-commerce.
Payment Flow:
Customer makes a card payment on the online store's platform.
Online store sends transaction data to the payment gateway.
Payment gateway directs the transaction to the acquirer chosen by the store.
Payment gateway sends transaction information to the online store.

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

Reversal Translation:
Definition: The refund of the amount of a completed transaction to the customer.
Reasons: Merchant error, fraud, etc.
Process: Request to the acquirer, investigation, refund of the amount.
Request deadline: Varies between 30 and 180 days.

Cancellation Translation:
Definition: Cancellation of an authorized but not yet completed transaction.
Reasons: Customer's withdrawal, error, product unavailability.
Process: Request to the acquirer before the transaction is finalized.
Amount not debited from the customer's account.

Fraud Translation:
Definition: Malicious action to obtain undue advantage in a transaction.
Types: Improper use of cards, unauthorized transactions, data forgery.
Impact: Financial losses, chargebacks, reputation damage, inconvenience.
Prevention: Security measures by acquirers, merchants, and customers.

Relationship between the Three:
Fraud is a common reason for reversals, especially via chargeback.
Fraud can lead to the cancellation of legitimate transactions.
Fraud prevention is crucial for all involved.

4. 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?

The conclusion that there are suspicious behaviors in the transactional data spreadsheet was based on a joint analysis of several factors, including:

Concentration of transactions in a short period of time: A large number of transactions occurring within a short timeframe, often indicating potential fraud or unauthorized activity.
High-value transactions at high-risk merchants: Transactions with unusually high amounts at merchants known to be associated with a higher risk of fraudulent activity.
Transactions across different devices: Transactions originating from multiple devices or locations, suggesting potential account takeover or card sharing.

Reversed transactions: A pattern of transactions being reversed or refunded, which may indicate fraudulent attempts to obtain goods or services without paying.

Based on the identified suspicious behaviors, I recommend the following actions:

Investigate the transactions in question: Conduct a thorough investigation of the flagged transactions to determine their legitimacy and identify any potential fraudulent activity.
Block the affected cards: Immediately block the cards associated with the suspicious transactions to prevent further unauthorized usage and protect cardholders.
Notify cardholders: Inform the cardholders of the suspicious activity and advise them to monitor their accounts closely for any unauthorized transactions.
Notify the relevant authorities: If fraud is suspected, report the incident to the appropriate authorities and cooperate with their investigations.

Additional Notes:

The specific actions taken should be tailored to the severity of the suspected behavior and the policies of the issuing bank or financial institution.
Implementing robust fraud prevention measures, such as transaction monitoring systems and cardholder authentication protocols, can help reduce the risk of fraudulent transactions.
Regularly educating cardholders about fraud prevention and encouraging them to report any suspicious activity promptly is crucial for maintaining account security.