

Task Report

Name: Caio T. Ladeira

Email: caiotladeira@gmail.com

Affiliation: Student at UFLA (Universidade Federal de Lavras)

Task 3.1

1. The Payment Ecosystem and Money Flow

Through this task, it became evident that the money flow relies on three core entities or pillars:

- **User (Cardholder):** The individual initiating the flow through daily purchases. Users consume multiple products and services from various merchants on a daily basis.
- **Merchant (Establishment):** The entity selling a product or service. Similar to the user, a merchant processes multiple sales to numerous individuals daily.
- **Bank:** The mediator of every transaction, present in every purchase to process payments.

Looking deeper into the banking and infrastructure layer, we can categorize the banks into three specific roles:

1. **Issuer (Issuing Bank):** The bank that issued the card to the consumer. They hold the consumer's funds and are responsible for authorizing or declining the transaction based on funds availability and fraud checks.
2. **Acquirer (Merchant Bank):** The financial institution that processes payments on behalf of the merchant. They enable the business to accept credit/debit cards and settle the funds into the merchant's account.
3. **Card Network (Scheme):** The infrastructure that connects all parties (e.g., Visa, Mastercard, American Express). They establish the rules, route the transaction data, and facilitate the clearing process.

The Dual Nature of the Flow:

- **Information Flow:** Occurs in fractions of a second. Since most transactions involve no physical cash, data points such as card number, account balance, price, and merchant ID must flow rapidly through the Card Networks and terminals. This data travels to servers and back to financial institutions for instant approval.
- **Money Flow (Settlement):** Unlike the information flow, the actual movement of funds typically takes 1–3 business days. Ultimately, the customer's bank transfers the money to the merchant's bank. During this process, acquirers generally earn revenue through service fees.

2. Roles and Integration in the Flow

- Acquirer: As previously defined, this is the major institution responsible for routing data to the networks and moving the actual money to the merchant.
- Payment Gateway: Mostly known as a card machine, this technology encrypts and transmits card data to the Acquirer and Issuer to verify the transaction. It serves as the integration point between the purchase action and the information flow.
- Sub-acquirer (Payment Facilitator): Often recognized as the entity where smaller businesses or users create accounts to receive payments. They act as an intermediary between the merchant and the Acquirer, aggregating transactions to simplify access to the payment system.

Integration Process:

- Information Flow: The Payment Gateway is the first step. It captures card details from the website/app, secures them, and passes them to the Acquirer for approval.
- Money Flow: The Sub-acquirer sits in the middle of the payout process. The Acquirer sends a bulk settlement to the Sub-acquirer, who then splits the funds and deposits the specific net amount into the merchant's account.

Task 3.2

1. Data Analysis: The complete analysis is presented in the attached file named "DataAnalysis".
2. Additional Data for Fraud Detection: To enhance the fraud detection model, the following data types would be highly relevant:
 - Geolocation Data: Capturing the location of the transaction (latitude and longitude). This enables the detection of physical inconsistencies, such as a card being used in two distant locations within a short timeframe (velocity checks).
 - Digital Footprint & History: Access to data regarding the last sites or apps where the user registered the card would be beneficial. Sites frequently associated with fraudulent purchase histories could be flagged as high-risk or suspicious.
 - Level 3 Data (Item Details): Detailed purchase information allows for model refinement based on behavioral analysis. For instance, identifying patterns where fraudulent activities focus on high-liquidity items, such as computer parts or smartphones, rather than low-risk goods.

Task 3.3

The solution and code for this task are provided in the files "DataAnalysis" and "SetupPrediction".