Anomaly Detection Credit Card

Anomaly detection in credit card transactions involves using statistical and Power BI techniques to identify unusual or fraudulent activities. The objective of this project is to develop a Power BI dashboard that provides insights into transaction patterns and detects potential anomalies, ensuring the security of credit card transactions.

Solution taken as Implementation:

It is a dashboard consisting of 3 primary section :

- **Home** : It consist of general information related to the dataset regarding fraud and non fraud insights.
  - **Total Transaction Amount (Card 📌) :**
    - SUM(Fraud[amount])
  - **Total Transaction Volume (Card 📌):**
    - Total_transact_count = COUNTA(Fraud[amount])
  - **Relation between Old Balance Org and Amount (Scatter Plot 📈) -**
    - This chart lets us **visually explore every data point**, revealing potential patterns and outliers that wouldn't be as apparent in other visualizations.

        - This **highlights potentially suspicious activity** where high spending doesn't match account history.
        - **Transaction Amount Over Time: Tracking Spikes and Drops(Line Chart 📈)**
            - This lets us **spot spikes and dips instantly**, like zooming in on a financial roller coaster.
            - This line chart whispers the story of spending habits, helping us **distinguish normal fluctuations from suspicious trends**.
    - **Average Transaction Values: Secure vs Fraudulent(Pie Chart 📈)**
        - It slices secure and fraudulent transactions like pizza, instantly showing their relative sizes.
        - This pie chart lets us compare values effortlessly, making it clear if fraudulent transactions are a minor blip or a significant concern demanding immediate attention.
- **Secure Transactions :** It consist of insightful information only related to secure transaction, which give an daily monitoring and information about secured transactions.
    - **Total Secure Amount (Card 📌):**
        - Total_normal_transact = SUMX(FILTER(Fraud,Fraud[isFraud] = 0), Fraud[amount])
    - **Total Secure Volume (Card 📌):**
        - Total_Normal_Count = COUNTAX(FILTER(Fraud,Fraud[isFraud] = 0),Fraud[Total_transact_count])
    - **Average Secure Amount (Card 📌):**
        - Avg_Secure_transaction = AVERAGEX(FILTER(Fraud,Fraud[isFraud] = 0),Fraud[amount])
    - **Max Secure Amount (Card 📌):**
        - highest_normal_transact_amount = MAXX(FILTER(Fraud,Fraud[isFraud] = 0), Fraud[amount])

- **% of Secure Amount (Card 📌):**
  - Percentage_Normal_transaction = DIVIDE([Total_Normal_Count], [Total_transact_count],0)*100
- **Understanding Secure Transaction Pattern by Transaction Type (Bar Chart 📈)**
  - It stacks up different transaction types like colorful towers, letting us compare their heights at a glance.
  - This chart helps us appreciate the normal patterns and pinpoint potential trouble spots, keeping our secure landscape healthy and robust.
- **Total Normal Volume by Time (Area Chart 📈)**
  - This visualization whispers the story of normalcy, highlighting potential shifts or unusual fluctuations.
- **Total Normal Amount by Transaction Type (Bar Chart 📈)**
  - Each type gets its own colorful block, stacked high or low based on its total value.
  - This visualization instantly shows which transaction types contribute the most to normal financial activity

- **Anomaly Alert :** It consist of insightful information only related to fraud, where the person can get quick detail ideas related to fraud, which can get identify to take action for more securing.
  - **Total Fraud Amount (Card 📌):**
    - Total_Fraud_transact = SUMX(FILTER(Fraud,Fraud[isFraud] = 1),Fraud[amount])
  - **Total Fraud Volume (Card 📌):**
    - Fraud_Tansact_Count = COUNTROWS(FILTER(Fraud,Fraud[isFraud] = 1))
  - **Average Fraud Amount (Card 📌):**
    - Avg_fraud_transaction = AVERAGEX(FILTER(Fraud, Fraud[isFraud] = 1), Fraud[amount])
  - **Max Fraud Amount (Card 📌):**

        - Highest_Fraud = MAXX(FILTER(Fraud,Fraud[isFraud] = 1),Fraud[amount])
    - **% of Fraud Amount (Card 📌):**
        - Percentage_fraud_transact = DIVIDE(Fraud[Fraud_Tansact_Count], [Total_transact_count],0) *100
    - **Customers with Multiple Fraudulent (Table 🗃️)**
    - **Top 5 Fraudulent Merchants (Table 🗃️)**
    - **Understanding Fraud Pattern by Transaction Type (Bar Chart 📈)**
        - It stacks up different transaction types like suspicious shadows, showing their heights at a glance.
        - This visualization reveals which transaction types harbor the most fraudulent activity.
    - **Fraud Transaction Volume by Time (Area Chart 📈)**
        - This visualization whispers the story of fraudulent trends, helping us identify specific timeframes to focus our defenses.
        - This bar chart empowers us to disrupt the fraudsters' schedule and keep them guessing.
    - **Top Fraud Transaction Amount by Transaction Type (Bar Chart 📈)**
        - Each type gets its own towering block, sized by the total stolen loot.
        - This visualization shines a bright light on the transaction types most susceptible to high-value fraud.

Key Insights

Overview:

- **Highly Secure Environment:** Over 99.94% of transactions were secure, highlighting the effectiveness of existing security measures.
- **Minimal Fraud Impact:** Fraudulent activity constitutes just 0.06% of both total transaction amount and volume, indicating successful fraud prevention efforts.
- **High-Value Targeting:** While fraud volume is low, the average and maximum fraud amounts are significant, suggesting potential targeting of larger transactions.

Secured Transactions:

- **CASH_OUT Dominance:** Cash withdrawals comprise 40.37% of all fraudulent transactions, indicating a preference for immediate cash access by perpetrators.
- **Step 0 vs. 1 Comparison:** Step 0 witnesses higher overall fraudulent amounts and average transaction values, but the gap widens for CASH_OUT transactions, where step 0 dwarfs step 1 by over $41 billion.
- **Normal Transaction Patterns:**
  - Cash withdrawals in normal transactions (isFraud 0) make up 35.50% of customer IDs.
  - Step 19 has the highest normal transaction volume (51,341), 155,478.79% higher than the lowest point.
  - Normal transaction volume varies significantly across all steps, indicating potential opportunities for targeted outreach or optimization.

Anomaly Alert:

- **Step 18 Red Flag:** This step saw the highest total fraudulent amount ($7.25 billion), 743,856.60% higher than the lowest point. Conduct a thorough investigation to understand the underlying factors.
- **Step 22: Fraud Hotspot:** This step has the highest fraudulent transaction volume (23), 1,050.00% higher than the lowest point. Identify and address vulnerabilities contributing to this concentration.
- **CASH_OUT and TRANSFER Targets:** These transaction types witness the highest number of fraudulent customers (197 for CASH_OUT, 186 for TRANSFER) and the highest individual fraud amount ($10 million). Implement stricter security measures for these transaction types.
- **Repeat Offenders:** Three customer IDs (C185805228, C200064275, C410033330) performed two fraudulent transactions each. Monitor and implement targeted prevention measures for these specific customers.

Recommendation:

- Conduct a dedicated investigation into **steps 18** and **22** to understand the vulnerabilities leading to concentrated fraud activity.

- Implement enhanced security measures for **CASH_OUT** and **TRANSFER** transactions, potentially including stricter verification, transaction limits, and real-time fraud detection.
- Continuously monitor fraud trends and adapt prevention strategies to stay ahead of evolving tactics.
- Develop step-specific mitigation plans based on identified vulnerabilities and fraud patterns.
- Invest in AI-powered fraud detection systems to learn from data and adapt in real-time.
- Implement proactive mitigation measures for identified repeat offenders, including stricter authentication and transaction limitations.
- Further analyze high-value fraud cases to understand the perpetrators' tactics and refine security measures.