**SAMPLE PROJECT-7**

**FINACIAL RISK ANALYSIS AND FRAUD DETECTION ﻿**

**(GOTLA SHIVANI YADAV)**

**AIM -What is the aim of analysis**

* Transaction Volume and Value Analysis
* Distribution of transactions across different merchant categories
* Distribution of transactions across different payment methods
* Fraud Detection
* **Demographic Analysis**
* **Risk Analysis**
* **Account Status Analysis**
* Trends in fraud cases over time and identify any seasonal patterns in fraud activities
* Fraud Type and Detection Method Analysis
* Resolution Analysis
* Resolution Analysis and its status of resolution

**FEATURES**

**4 data sheets were collected**

**1.** **Transaction Data Sheet**

**Transaction ID:** A unique identifier for each transaction.

**Customer ID:** A unique identifier for each customer involved in the transactions.

**Transaction Amount:** The amount of money involved in the transaction.

**Transaction Date:** The date on which the transaction took place.

**Merchant Category:** The category of the merchant where the transaction occurred (e.g., Electronics, Entertainment, Travel, Food).

**Payment Method:** The method of payment used for the transaction (e.g., JCB 15-digit, VISA 19-digit, VISA 16 digit).

**Risk Score:** A numerical score indicating the risk level of the transaction, with higher values indicating higher risk.

**Fraud Flag:** A binary flag indicating whether the transaction was identified as fraudulent (1) or not (0).

**2.** **Customer Profiles Sheet**

**Customer ID:** A unique identifier for each customer.

**Name:** The name of the customer.

**Age:** The age of the customer.

**Gender:** The gender of the customer.

**Credit Score:** The credit score of the customer.

**Risk Category:** The risk category assigned to the customer (e.g., Low, High).

**Annual Income:** The annual income of the customer.

**Account Status:** The current status of the customer's account (e.g., Active, Inactive)

**3. Fraud Cases Sheet**

**Fraud CaseID:** A unique identifier for each fraud case.

**Transaction ID:** The identifier of the transaction associated with the fraud case.

**Fraud Type:** The type of fraud detected (e.g., Card Not Present, Identity Theft, Skimming).

**Detection Method:** The method used to detect the fraud (e.g., Machine Learning, Manual Review).

**Reported Date:** The date on which the fraud was reported.

**Resolution Status:** The current status of the fraud case (e.g., Pending, Resolved, Investigating).

**4. AML Compliance Sheet**

**AML Case ID:** A unique identifier for each Anti-Money Laundering (AML) case.

**Customer ID:** The identifier of the customer involved in the AML case.

**Transaction ID:** The identifier of the transaction associated with the AML case.

**AML Alert Level:** The alert level of the AML case (e.g., Low, Medium, High, Critical).

**Review Status:** The status of the review for the AML case (e.g., Reviewed, Not Reviewed).

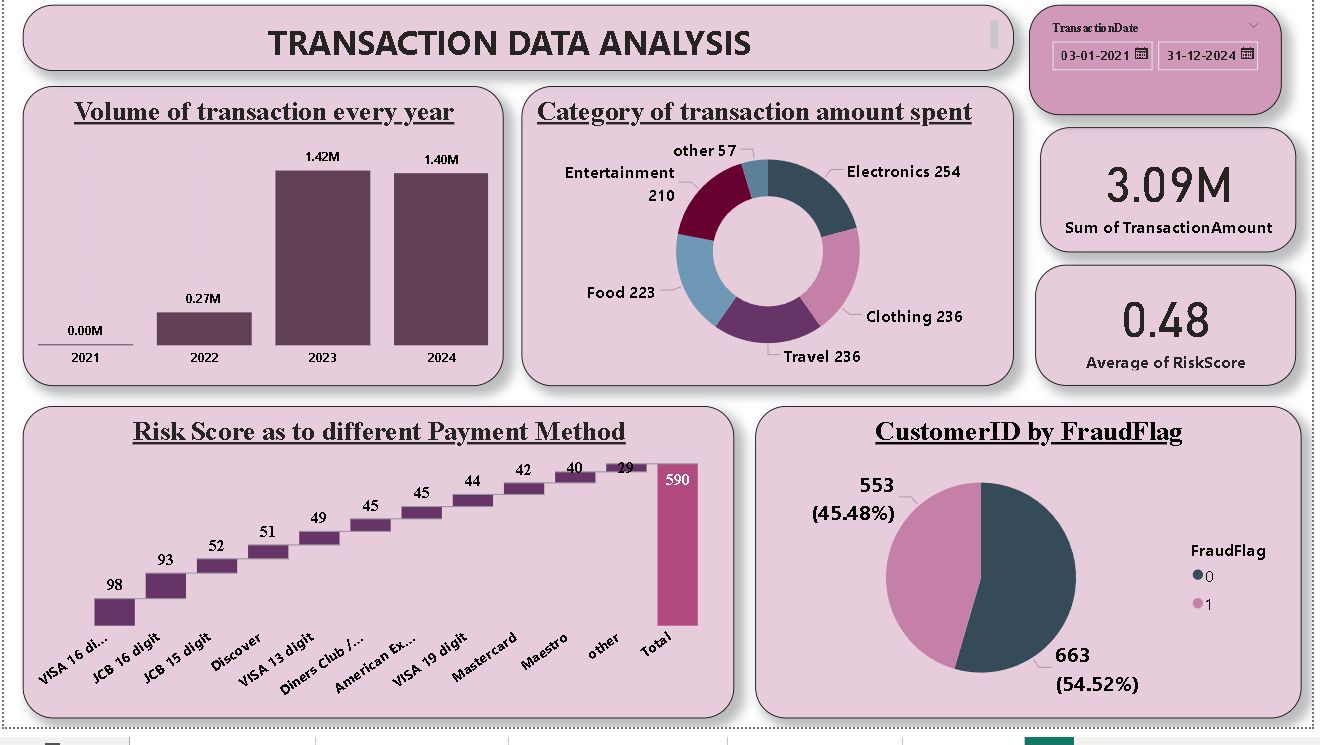
**Alert Date:** The date on which the AML alert was generated.

**METHODOLOGY**

* Data collection – data is collected for the following metrices
* Data cleaning – data is cleaned with the use of SQL – where the null values of numerical are replaced with the mean values and categorical values are replace with the mode. There by the outliers are removed and values recording is done.
* Summary statistics – summary statistics is done in excel using data analysis tool
* Data Modelling – data modeling is done in model view of power bi
* Data analysis – the data cleaned is analyses using Power BI with various charts and give meaning full insights

**OUTPUT**

**Summary of TRANSACTION DATA ANALYIS**

****

•  **Transaction Volume and Value Analysis:**

1. Total number of transactions took place and number of transactions over time is analyzed. here the volume of transactions is more in the year 2023 there by 2024 then 2022 and 2021
2. Identify peak transaction periods by adjusting the slicer for days, months.

•**Distribution of transactions across different merchant categories where** the category of electronics occupies the more share and there by clothing and travel takes of 2 places

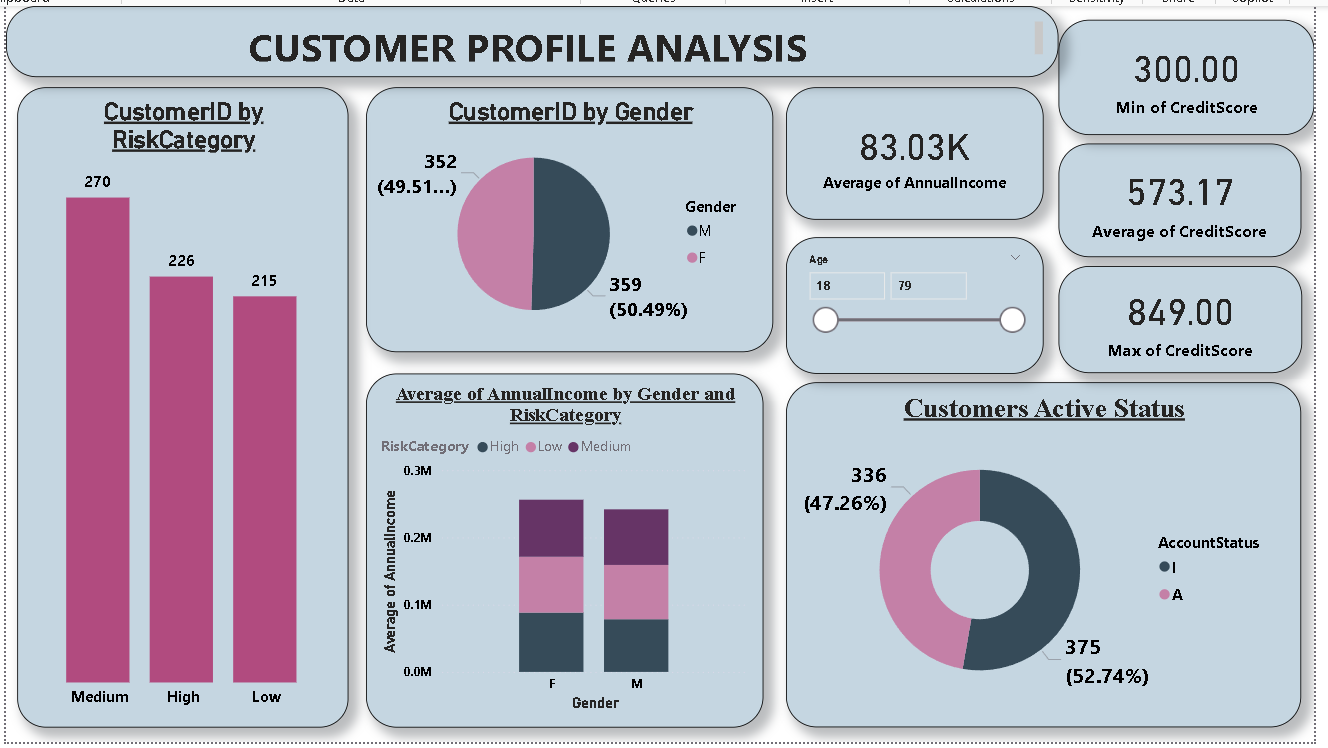
•**Distribution of transactions across different payment methods** where payment through VISA 16 digit is termed to be highest there by JCB 16 digit.

•Analysis of **the relationship between merchant categories and risk scores** like if we click on electronics, it shows how much risk score is occurred

**• Fraud Detection:**

1. Number of flagged fraudulent transactions here 1 depicts as active and 0 depicts the inactive rate although here inactive rate is high and active is of low percentage coverage
2. Fraud rate per merchant category or payment method can also be analyzed by clicking on the category or payment method required.

**SUMMARY OF CUSTOMER PROFILE ANLYSIS**



**Demographic Analysis:**

* Age and gender distribution of customers can be analyzed
* Analyze income levels across different age groups or genders.

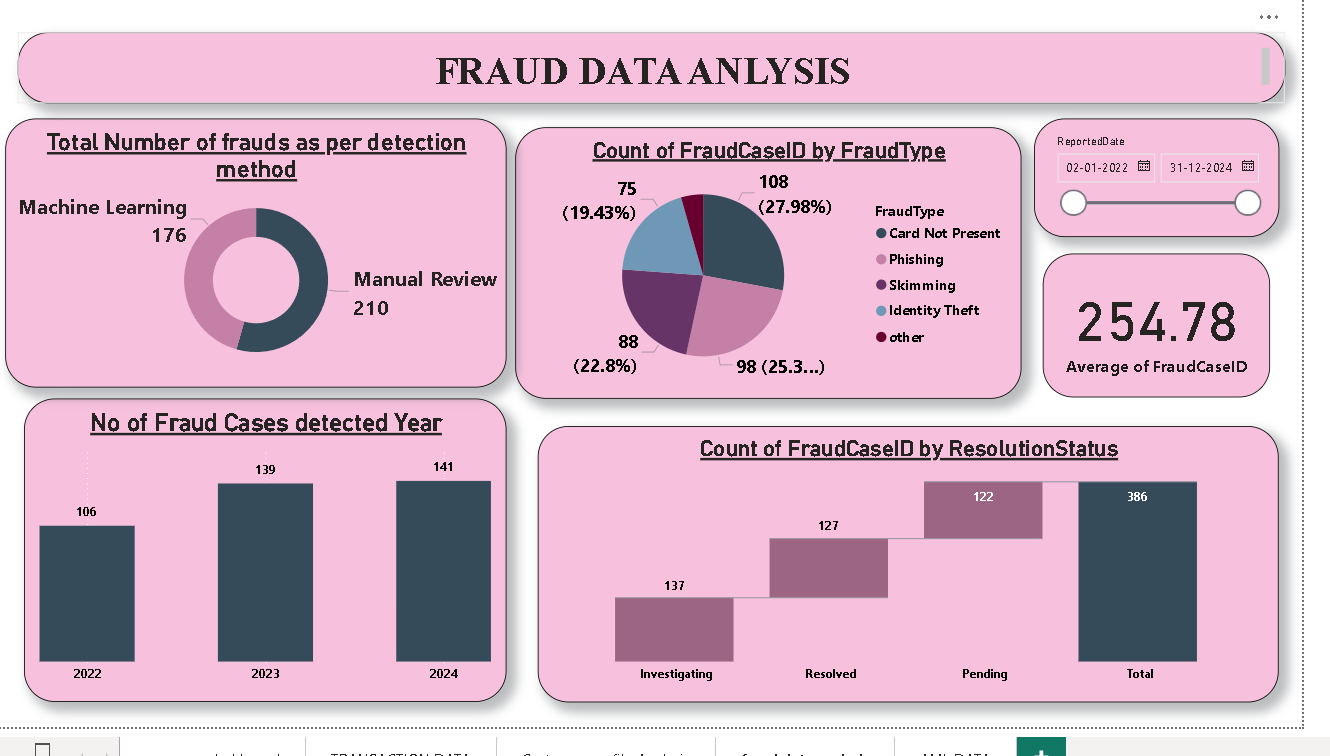
**Risk Analysis:**

* **Analyze the risk category up to how many customers fall in to it which risk category so here it is observed that most of the customer fall into medium risk category and high.**
* Distribution of credit scores and their relation to risk categories a slicer is introduced to analyses accordingly.

**Account Status Analysis:**

* Proportion of active versus inactive accounts. In active is termed as high here.
* Analyze the relationship between account status and customer demographics or credit scores.

**SUMMARY OF FRAUD ANALYSIS**

****

**Fraud Type and Detection Method Analysis:**

* Distribution of different types of fraud occurred
* Effectiveness of different detection methods here it is machine learning vs. manual review. here manual review has its highest share of identifying fraud

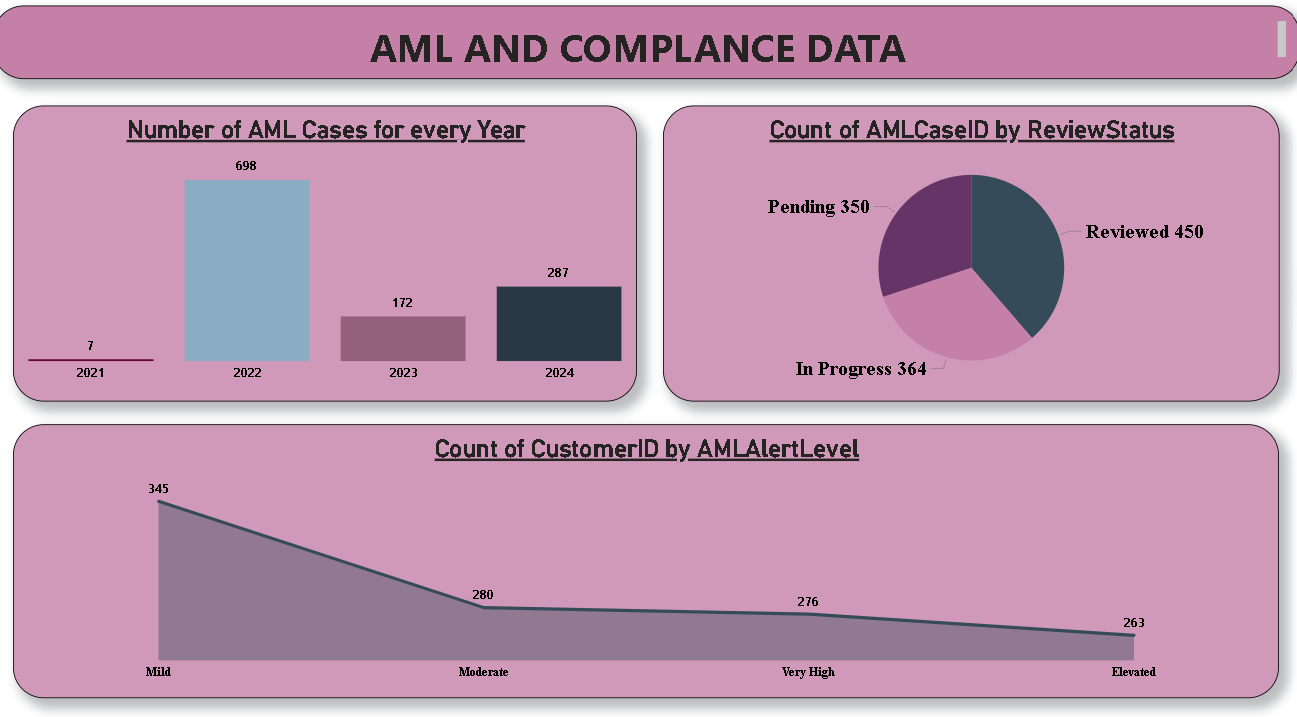
**Resolution Analysis**

* Status of fraud case resolutions pending, resolved or investigating it is observed that resolved and investigation takes a higher share than left pending

**Temporal Analysis:**

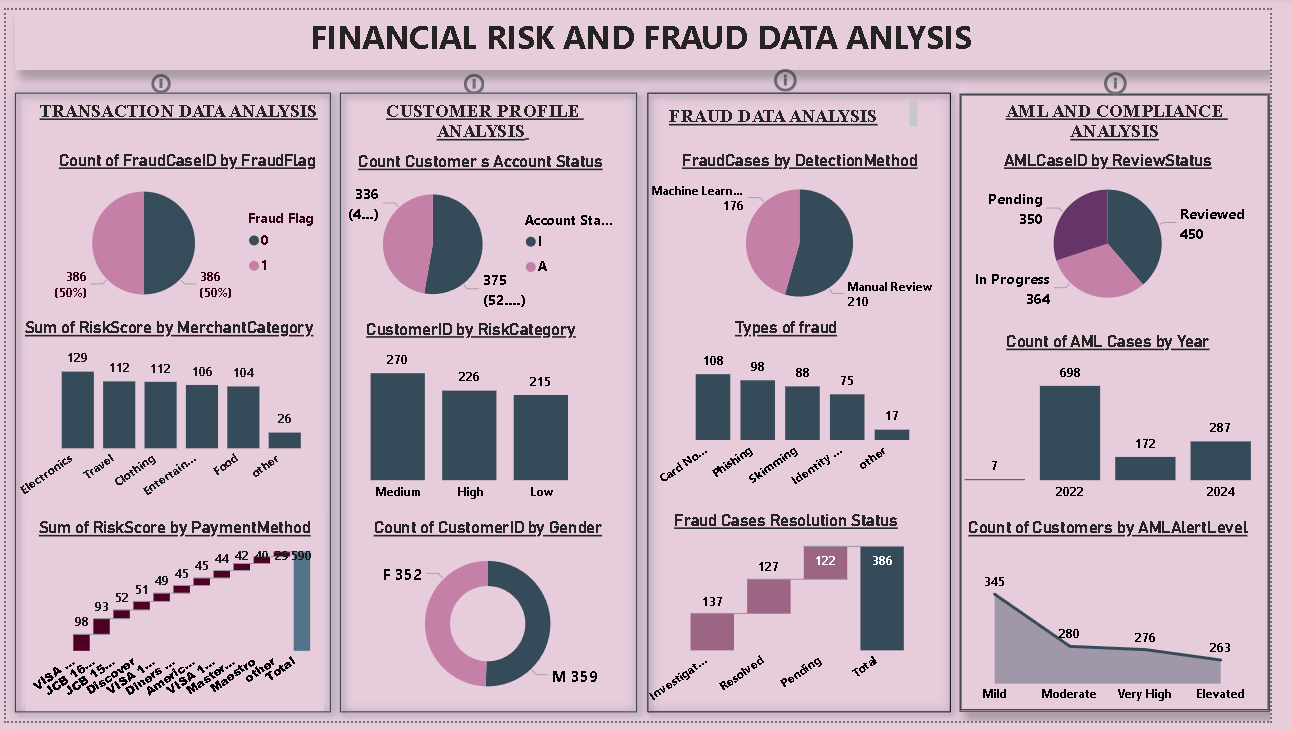
* Trends in fraud cases over time (monthly or quarterly) highest no of frauds is analyzed in the year 2024
* Identify any seasonal patterns in fraud activities.

**SUMMARY OF AML AND COMPLIANCE DATA**



* **Alert Level Analysis:** Distribution of AML alerts by alert level (Moderate, Very High, etc.). Analyze the relationship between alert levels and review statuses.
* **Review Status Analysis**: Current status of AML case reviews is Reviewed, Pending or In Progress
* **Customer-Level Analysis:** Number of AML alerts per customer.

**SUMMARY DASHBOARD – OVERALL SUMARRY**



* **Transaction Data Analysis:**

Risk Scores: Higher risk scores are observed in Electronics and Travel merchant categories, along with payment methods like Card Network and Phishing.

Fraud Cases: A significant portion of fraud cases are categorized as "Other," indicating potential new or emerging fraud types.

* **Customer Profile Analysis:**

Account Status: The majority of customers have active accounts, with a smaller percentage closed or inactive.

Risk Category: A balanced distribution of customers across medium, high, and low-risk categories is observed.

Gender: The customer base is evenly split between females and males.

* **Fraud Data Analysis:**

Detection Method: Machine Learning plays a dominant role in fraud detection, followed by manual review.

Fraud Types: Phishing and Skimming are the most prevalent fraud types.

Resolution Status: A significant portion of fraud cases remain pending investigation.

* **AML and Compliance Analysis:**

Review Status: A substantial number of AML cases are still under review, indicating potential bottlenecks in the investigation process.

Cases by Year: A slight increase in AML cases is observed in 2024 compared to 2022.

Customer Alert Levels: A concerning number of customers fall into the "Very High" alert level category, requiring immediate attention.

**CONCLUSION**

The overall analysis highlights areas of concern, such as emerging fraud types, a high volume of pending AML cases, and a significant number of customers with high alert levels. It also provides valuable insights into customer profiles, transaction patterns, and fraud trends, enabling informed decision-making and risk mitigation strategies.