CREDIT CARD FRAUD DETECTION

1.Business Understanding

Context:

In the ever-evolving landscape of digital finance, Mastercard, a leading global credit card provider, has observed a worrying increase in fraudulent transactions over the past year in Europe. These fraudulent activities not only result in substantial financial losses but also erode customer trust and can potentially damage the company's reputation.

Stakeholder:

The primary stakeholder is the Fraud Detection Department at Mastercard, led by the Chief Risk Officer (CRO), Sam Miller. The department is responsible for minimizing fraud losses and maintaining customer trust by accurately detecting and preventing fraudulent credit card transactions.

Business Problem:

The department has historically relied on rule-based systems to flag potentially fraudulent transactions. However, this method has proven inadequate due to its high rate of false positives(legitimate transactions mistakenly blocked as fraud)which has led to customer dissatisfaction and a surge in service calls. Additionally, the rule-based system fails to catch more sophisticated frauds, leading to false negatives (actual fraud that goes undetected.)

Challenge:

The challenge for the Fraud Detection Department is twofold:

1. Reduce False Positives: Lower the rate of legitimate transactions being incorrectly flagged as fraudulent to improve customer satisfaction and reduce operational costs associated with service calls.

2. Reduce False Negatives: Increase the detection rate of actual fraudulent transactions to prevent financial losses and safeguard the company's and customers' assets.

Machine Learning Solution:

To address these challenges, the department is looking to leverage machine learning (ML) models capable of learning from historical transaction data. The goal is to develop a predictive model that can more accurately identify fraudulent transactions than the existing rule-based system, adjusting to new patterns as fraudsters' tactics evolve.

Objective:

The immediate objective is to select and fine-tune an ML model that can strike an optimal balance between precision (minimizing false positives) and recall (minimizing false negatives), given the dataset's unbalanced nature.

Expected Outcome:

By successfully implementing a machine learning solution, Mastercard expects to:

- Enhance customer experience by reducing the rate of transaction interruptions due to false fraud alerts.

- Strengthen security measures by accurately identifying and preventing more fraudulent activities.

- Decrease the operational costs associated with manual transaction reviews and customer support for false fraud claims.

- Uphold the company’s reputation as a secure and customer-friendly credit card provider.

Next Steps:

The Fraud Detection Department, under the guidance of the CRO, will collaborate with the Data Science team to develop, train, and deploy the selected machine learning model. Continuous monitoring and model updates will ensure the system remains effective against emerging fraud techniques.

2.Data Understanding

Dataset

Source; Kaggle

The dataset at hand is a record of credit card transactions over two days in September 2013 from European cardholders. It includes 284,807 transactions, of which 492 are fraudulent. This indicates a severe class imbalance, with fraud cases representing only about 0.172% of the total transactions.

Features

The data comprises numerical input variables which are the result of Principal Component Analysis (PCA) transformations named V1 through V28. Due to confidentiality, the original features before PCA transformation are not provided. This anonymization ensures privacy but limits domain-specific analysis and feature engineering.

The dataset also includes two features not subjected to PCA:

- `**Time**`: The seconds elapsed between each transaction and the first transaction in the dataset.

- `**Amount**`**:** The transaction amount, which could be a critical feature as transaction size may be indicative of fraudulent activity.

The target variable, `**Class**`, indicates whether each transaction is fraudulent (`1`) or not (`0`).

Class Imbalance:

Given the substantial imbalance in the dataset, standard accuracy metrics could be misleading. A model could naively predict all transactions as non-fraudulent and still achieve high accuracy. Therefore, the evaluation will focus on metrics that provide more insight into the performance on the minority class, such as the Precision-Recall Curve (AUPRC), F1 score, and Confusion Matrix.

Data Quality:

The dataset is well-prepared with no missing values. However, the PCA transformation makes it difficult to perform certain data quality checks that rely on understanding the actual scale and distribution of the data.

Initial Insights:

- Fraudulent transactions are rare, which aligns with real-world expectations of fraud occurrence.
- Due to PCA, the features are orthogonal, ensuring there is no multicollinearity within these variables.
- The 'Time' and 'Amount' features may require scaling or normalization to align with the PCA components.
- Feature 'Class' is highly imbalanced, necessitating specialized techniques for training and evaluating models.

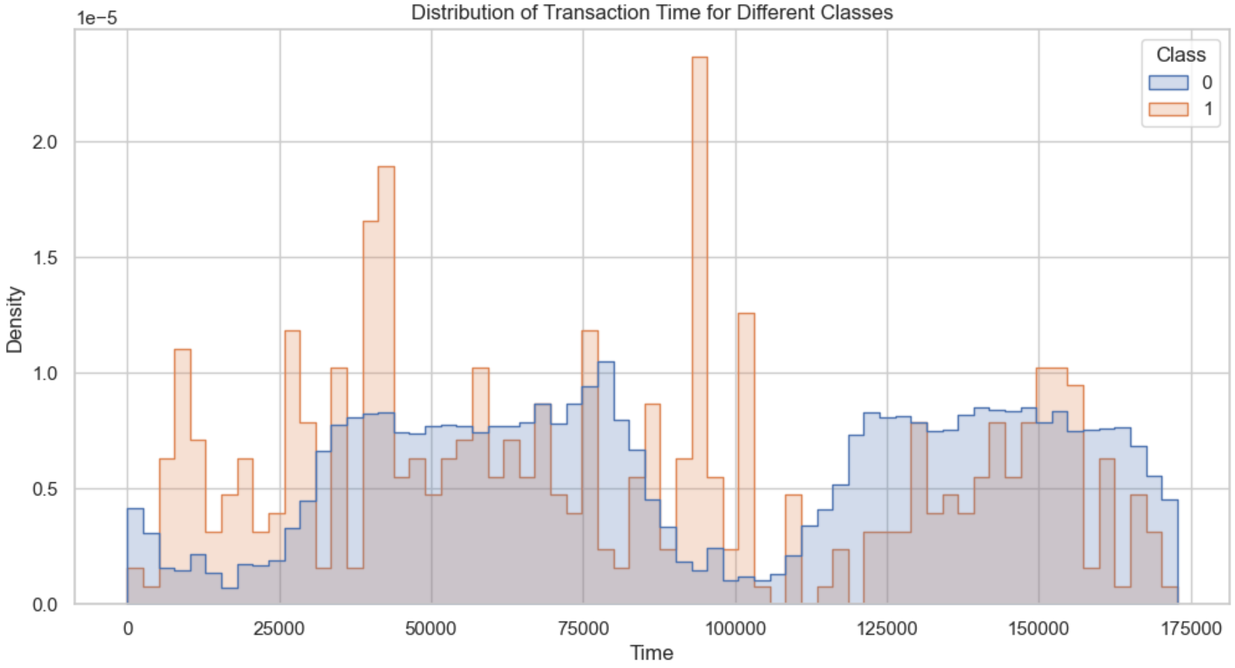
Potential Challenges:

- The anonymized nature of PCA-transformed features prevents us from extracting domain-specific insights.
- The model needs to be sensitive enough to detect the minority class effectively while not overwhelming the system with false positives.
- The imbalance may require resampling techniques or specialized algorithms that can handle skewed class distributions.

Conclusion

Understanding this dataset is fundamental for creating a predictive model that can effectively identify fraudulent transactions. Moving forward, the modeling approach must carefully consider the balance between detecting fraud (recall) and maintaining user experience by minimizing false alarms (precision). The next phase will involve exploratory data analysis, feature engineering (if possible, with the PCA components), and preparing the data for modeling with a focus on addressing the class imbalance issue.

Effective Exploratory Data analysis for classification



The distribution plots for the 'Time' and 'Amount' features provide some interesting insights

Transaction Time Distribution

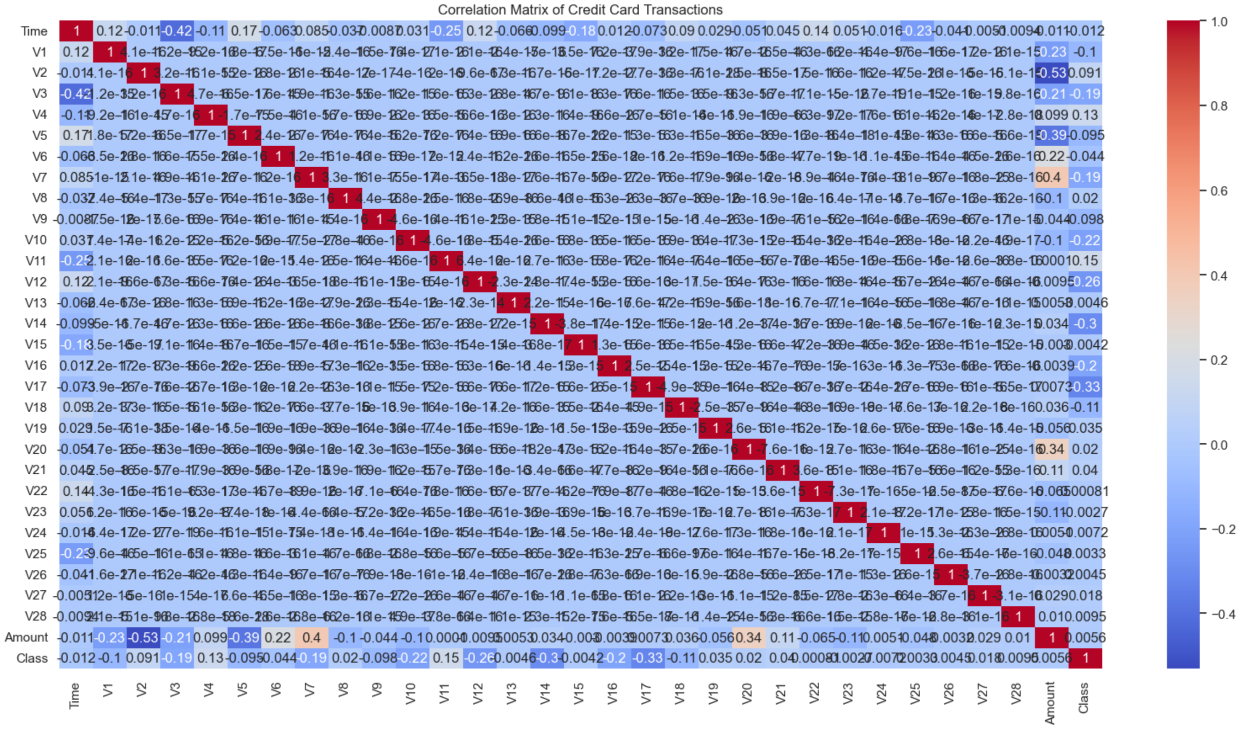
- The distribution of transactions (both fraudulent and non-fraudulent) over time shows cyclic patterns, likely reflecting daily activity cycles.

- There doesn't appear to be a clear, distinct pattern in the timing of fraudulent transactions compared to non-fraudulent ones. However, there might be slight increases in fraudulent activity at certain times.

Transaction Amount Distribution:

- Most transactions, regardless of class, are of lower amounts, with the distribution heavily skewed towards smaller values.

- Fraudulent transactions also tend to be of lower amounts, note that the scale of fraudulent transactions is much smaller due to the class imbalance.



The correlation analysis reveals the following

Correlation of 'Time' with 'Class'

- The correlation coefficient is approximately -0.0123, indicating a very weak inverse relationship between the time of the transaction and its likelihood of being fraudulent.

Correlation of 'Amount' with 'Class'

- The correlation coefficient is about 0.0056, suggesting a very weak positive relationship between transaction amount and the likelihood of fraud.

Correlation of PCA Components with 'Class':

- Some of the PCA-transformed features (like V17, V14, V12) have higher negative correlations with the 'Class' variable. This suggests they might be more significant in predicting fraud.

- Features like V11 and V4 show a moderately positive correlation with the 'Class' variable.

From these observations, it's clear that neither 'Time' nor 'Amount' has a strong linear relationship with fraud occurrence. However, considering the nonlinear and complex nature of such transactions, these features could still be valuable in a predictive model, especially when combined with the PCA-transformed features.

3.Modeling

The department considered various ML models, namely:
- Logistic Regression
- Random Forest
- Gradient Boosting

Evaluation

Logistic Regression Results

- ***Accuracy***: 97.32%
- ***Precision:*** 5.23%
- ***Recall:*** 92.65%
- ***F1 Score***: 9.91%
- ***AUPRC***: 79.5%

Random Forest Results

- Accuracy: 99.95%
- Precision: 83.22%
- Recall: 87.50%
- F1 Score: 85.30%

-AUPRC: 88.35%

Gradient Boosting Results

- Accuracy: 99.35%
- Precision: 18.56%
- Recall: 91.18%
- F1 Score: 30.85%
- AUPRC: 78.14%

Recommendations

- Deploy Logistic Regression as an initial filter followed by Random Forest for better precision and recall.

- Explore unsupervised learning and deep learning techniques for improved detection.
- Continuous model monitoring and updates are crucial for adapting to evolving fraud patterns.

Evaluation

The Logistic Regression and Random Forest models were selected for deployment due to their superior performance.

Deployment

Pickling Models

- Logistic Regression Model: Saved as 'logistic_regression_model.pkl'.
- Random Forest Model: Saved as 'random_forest_model.pkl'.