# CS379 Unit 3 Individual Project: Credit Card Fraud Detection

Jacob Marquez

Colorado Technical University

# Table of Contents

## Introduction

In the modern age of digital transactions, credit card fraud has rapidly emerged as a menacing shadow over the realm of e-commerce and electronic banking. The anonymity that the internet provides has given malicious actors the tools to exploit unsuspecting victims, wreaking havoc on personal finances and undermining trust in financial institutions. As the volume of online transactions continues to grow exponentially, so does the urgency to develop robust methods for detecting and preventing these fraudulent activities. This paper embarks on an exploration of credit card transaction data, harnessing the power of the Random Forest algorithm. Through this analysis, I aim to demonstrate patterns and characteristics inherent to fraudulent transactions, providing insights that could lead to enhanced security measures and a safer transaction environment for all.

## Initial Analysis

The first step was to analyze the data contained in the ARFF dataset provided. Upon inspection of the first few rows, a clear understanding of the data's structure was gained, and I was able to begin structuring the model. For more efficient data handling, byte strings were subsequently converted to regular strings. Furthermore, in the target variable 'class', string values "good" and "fraudulent" were mapped to their numerical counterparts, `0` and `1`, respectively.

## Data Preprocessing

In the dataset, both categorical and numerical features were identified. To address these, a preprocessing pipeline was established. For the numerical features, missing values were filled using the mean, followed by standard scaling. Meanwhile, for the categorical features, missing values were addressed by substituting them with the most frequent value, after which one-hot encoding was applied.

**Model Training and Evaluation**

The dataset was divided into training, validation, and test sets. Subsequently, the Random Forest model was trained using the data from the training set. Upon evaluation of the model on the validation set, I provided metrics such as precision, recall, and F1-score for both classes. Here are those results:

**RFM Data Preprocessing Results**

*Good Transactions (Class 0):*
Precision: 0.75
Recall: 0.89
F1-Score: 0.82

*Fraudulent Transactions (Class 1):*
Precision: 0.56
Recall: 0.31
F1-Score: 0.40

*Overall Accuracy:* 72%

The model has an Overall Accuracy of 72% but the recall for fraudulent transactions is 31%, which means it detects only 31% of the actual fraudulent transactions in the validation set. This is a concern, as a significant portion of actual fraud is going undetected. We will hopefully improve this score to catch more fraudulent activity, however, there is an important balance at play here. We want to avoid false accusation but catch as much fraudulent activity as possible.

**Oversampling**

In an effort to enhance the recall for the fraudulent class, manual oversampling of the minority class, which represents fraudulent transactions, was implemented to achieve a balance between the classes. Following this adjustment, the Random Forest model was retrained using the oversampled training data. While there was a noticeable improvement in the recall for the fraudulent class as a result, the performance still did not reach an optimal level.

**RFM Oversampling Results**

*Good Transactions (Class 0):*
Precision: 0.76
Recall: 0.83
F1-Score: 0.79

*Fraudulent Transactions (Class 1):*
Precision: 0.50
Recall: 0.40
F1-Score: 0.44

*Overall Accuracy:* 70%

While the recall for fraudulent transactions has improved slightly to 40% (from 31% before oversampling), it's still relatively low. This means that 60% of actual fraudulent transactions in the validation set are going undetected. Extra measures should be taken to improve the percentage of detected fraudulent transactions.

**Stratified Sampling and Adjusting the Classification Threshold**

To further bolster model performance, Stratified Sampling and Adjusting the Classification Threshold were proposed as potential methods. The rationale behind this approach is that Stratified Sampling ensures that the dataset maintains the same proportion of classes as the original, thus providing a more representative sample for training. Additionally, by adjusting the classification threshold, we can control the trade-off between false positives and false negatives, offering a more tailored classification outcome based on the specific needs of the problem at hand. While these modifications did lead to an increase in recall, an accompanying drop in precision was observed.

**RFM Stratified Sampling & Adjusted Classification Threshold Results**

*Good Transactions (Class 0):*
Precision: 0.84
Recall: 0.56
F1-Score: 0.67

*Fraudulent Transactions (Class 1):*
Precision: 0.42
Recall: 0.75
F1-Score: 0.54

*Overall Accuracy:* 62%

By using stratified sampling and adjusting the classification threshold, we have significantly improved the recall for fraudulent transactions (class 1) to 75%. However, it's essential to note that while recall has improved, precision for fraudulent transactions has dropped to 42%, indicating a higher number of false positives. We could improve the precision on fraudulent transactions by incorporating Cost-sensitive Learning.

## Cost-sensitive Learning

To address the imbalance in data representation, cost-sensitive learning was employed by assigning specific weights to classes within the Random Forest model. This approach emphasized the fraudulent class, giving it more importance in the learning process. The underlying premise is that by making the model more sensitive to the cost of misclassifying specific classes, especially the minority class, it can potentially improve its ability to correctly classify those underrepresented instances. As a result of this strategy, an improvement in precision for the fraudulent class was observed but the recall decreased again.

### RFM Cost-sensitive Learning Results

*Good Transactions (Class 0):*
Precision: 0.74
Recall: 0.94
F1-Score: 0.83

*Fraudulent Transactions (Class 1):*
Precision: 0.61
Recall: 0.23
F1-Score: 0.33

*Overall Accuracy:* 0.73

While the precision for fraudulent transactions has improved slightly, the recall was reduced sharply and remains at a relatively low 23%. This means that 77% of actual fraudulent transactions in the validation set are going undetected. Further adjustments would be needed to increase the recall for class 1 while trying to maintain a reasonable precision. Another option that may yield more favorable results would be to tackle this problem using another model such as Gradient Boosted Trees or algorithms with built-in class weight adjustments.

## Conclusion

In the constantly evolving landscape of digital transactions, the challenge of effectively detecting and combating credit card fraud remains paramount. This study employed the Random Forest algorithm to delve into the intricacies of credit card transaction data and discover patterns characteristic of fraudulent activities. While the model demonstrated promise in discerning legitimate from illicit transactions, it was made apparent that achieving an optimal balance between recall and precision, especially for the fraudulent class, was non-trivial. Various techniques, including Oversampling, Stratified Sampling, and Cost-sensitive Learning, were deployed in an attempt to enhance model performance.

While oversampling and adjusting the Classification Threshold improved recall, they did so at the expense of precision. This suggests that if a problem context permits a higher rate of false positives, then these methods might be the optimal solution. On the other hand, if the aim is to strike a balance without incurring too many false positives, relying solely on Oversampling might be the better choice. The exploration into Cost-sensitive Learning hinted at potential, but it became evident that more extensive testing or a larger dataset might be needed to yield a more optimal result.

In summation, the best approach largely hinges on the specific objectives set for the problem. While this study has made steps in the right direction, further research, and exploration, possibly with other algorithms or more data, could provide more comprehensive solutions to the pressing issue of credit card fraud.

## References

Bhattacharyya S, Jha S, Tharakunnel K, Westland JC. Data mining for credit card fraud: A comparative study. *Decision Support Systems*. 2011

Dal Pozzolo A, Caelen O, Le Borgne YA, Waterschoot S, Bontempi G. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert systems with applications*. 2014

Breiman L. Random forests. *Machine learning*. 2001

Chawla NV, Bowyer KW, Hall LO, Kegelmeyer WP. SMOTE: synthetic minority over-sampling technique. *Journal of artificial intelligence research*. 2002

He H, Bai Y, Garcia EA, Li S. ADASYN: Adaptive synthetic sampling approach for imbalanced learning. *In 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*. IEEE. 2008

Elkan C. The foundations of cost-sensitive learning. *In Proceedings of the 17th international joint conference on Artificial intelligence*. 2001