# Capstone Credit Card Fraud Detection

Sudarsan “Sudi” Narasimhan

I. **Business Problem**

In the modern world, commercial transactions and business that were once conducted through paper and physical means are quickly being replaced through digital and electronic means. Instead of a printed financial note that is exchanged between two or more parties, the exchange occurs as electronic and paperless transactions, at sub second speeds, and sometimes involving bad actors who intend to intercede in these transactions to commit fraud. The goal of this exercise is to identify, through different AI/ML classification models, whether a transaction is fraudulent or not. The goal would be to set up a set of independent variables that would form the ‘X’ component in the model, and a ‘Y’ dependent variable that would determine whether a transaction is fraudulent conducted through bad intent.

II **Situation Assessment**

Resources employed for this exercise will include a Kaggle Credit Card dataset with 284000 + instances, The goal is to compare the performance of the classifiers (k-nearest neighbors, logistic regression, decision trees, and support vector machines), and thereby assess which type of classification model best identifies whether a transaction is fraudulent or not. Metrics that will best identify include accuracy, Precision, Recall, F-1-score among others. Through the most optimal model, the classification model will be able to predict a set of fraudulent vs. non-fraudulent transactions. Naturally, there will be True Positives, False Positives, False Negatives, and True Negatives. Ultimately, as stated in the problem statement, AI/ML when employed to identify fraudulent transactions can help in optimizing business resources, ensuring that only the most genuine transactions are committed, and prevent fraudulent transactions from committing theft and disrupting customer experience and business operations.

## K Nearest Neighbors Classifier

A screenshot of a computer screen

Description automatically generated

A screenshot of a graph

Description automatically generated

A screenshot of a graph

Description automatically generated

* True Negatives – 1452 – The number of non-fraudulent transactions that were correctly identified as such.
* False Positives – 6 The number legitimate transactions that were misclassified as fraudulent.
* False Negatives – 12 The number of fraudulent transactions that were misclassified as legitimate when they should have been classified as fraudulent.
* True Positives – 130 – The number of fraudulent transactions classified accurately as fraudulent.
* Accuracy – Model, with 98.88%, has a high probability of classifying both fraudulent and non-fraudulent transactions.
* High Precision – When a model predicts a transaction as fraudulent, it is accurate 95.66% of the time. As such there are few false positives, reducing the potential for classifying legitimate transactions as fraudulent.
* High Recall – The model detects 91.5% of all fraudulent transactions leaving approximately 8+% of the fraudulent transactions not detected by the model.
* Strong measure F1-Score and High Specificity with a good balance of precision and recall, and an effective way of identifying non-fraudulent transactions.

## Logistic Regression

A white background with black text

Description automatically generated

A screenshot of a graph

Description automatically generated

A screenshot of a graph

Description automatically generated

* True Negatives – 1443 – The number of non-fraudulent transactions that were correctly identified as such.
* False Positives – 15 -The number legitimate transactions that were misclassified as fraudulent.
* False Negatives – 47-The number of fraudulent transactions that were misclassified as legitimate when they should have been classified as fraudulent.
* True Positives – 95 – The number of fraudulent transactions classified accurately as fraudulent.
* Accuracy – The model is very effective in identifying and classifying most of the transactions.
* High level of Precision – Although not as high as in K-Nearest Neighbors, there’s still significant precision whereby if the model predicts a transaction is fraudulent, it is correct 86.4% of the time.
* Average Recall – Model correctly identifies 66.8% of the fraudulent transactions leaving 44% as not identifying fraudulent transactions
* Moderate F1- score of 75% indicating a good balance of precision and recall.
* High Specificity of 99% indicating that it is excellent at identifying legitimate transactions.

## Support Vector Machine (SVM)

A screenshot of a graph

Description automatically generated

After GridSearch:

A screenshot of a computer

Description automatically generated

A screenshot of a graph

Description automatically generated

* True Negatives – 2185 – The number of non-fraudulent transactions that were correctly identified as such.
* False Positives – 7 The number legitimate transactions that were misclassified as fraudulent.
* False Negatives – 53- The number of fraudulent transactions that were misclassified as legitimate when they should have been classified as fraudulent.
* True Positives – 155 – The number of fraudulent transactions classified accurately as fraudulent.
* Accuracy - High level of accuracy with 97.5% suggesting that the model can correctly classify most transactions.
* High Level of Precision with 96%, indicating that when a model predicts a transaction as fraudulent, it’s accurate 96% of the time.
* Moderate recall with 74.5% such that the model correctly identifies 74.5% of all fraudulent transactions.
* F1 Score of 84.4% reflects a good balance between precision and recall.
* High specificity of 99.7% indicating that it correctly identifies legitimate transactions.

## Decision Tree Classifier

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a graph

Description automatically generated

* True Negatives – 2190 – The number of non-fraudulent transactions that were correctly identified as such.
* False Positives – 2- The number legitimate transactions that were misclassified as fraudulent.
* False Negatives – 1- The number of fraudulent transactions that were misclassified as legitimate when they should have been classified as fraudulent.
* True Positives – 207 – The number of fraudulent transactions classified accurately as fraudulent.
* The model is highly accurate at 99.9% with the strongest ability of classifying transactions.
* High Precision of 99% indicating that when a model predicts a transaction as fraudulent, it’s correct 99% of the time.
* High Recall such that the model detects 99.5% of all fraudulent transactions.
* High F1 score of 99.2% indicating a high balance of precision and recall.
* High specificity of 99% indicating model is very effective at correctly identifying non-fraudulent transactions.

**Deep Learning Results**

A yellow and purple squares with numbers

Description automatically generated

* True Negatives – 1451 – The number of non-fraudulent transactions that were correctly identified as such.
* False Positives – 7- The number legitimate transactions that were misclassified as fraudulent.
* False Negatives – 9- The number of fraudulent transactions that were misclassified as legitimate when they should have been classified as fraudulent.
* True Positives – 133 – The number of fraudulent transactions classified accurately as fraudulent.
* The model is very accurate at 99%
* Precision is at 95% indicating that 95% of the transactions that are labelled as fraudulent are actually so.
* Recall in this case is 93% indicating that 7% of the transaction that were fraudulent wasn’t captured by the model.

A graph with blue bars

Description automatically generated

* The most important features that are correlated to a fraudulent transaction include ‘ratio to median purchase price’, ‘online order’, and ‘distance from home’.

**Summary**

By leveraging a decision tree classifier, the core customer can deploy this model to identify fraudulent transactions thereby improving productivity, reducing costs associated with liability, and driving customer assurance that electronic transactions can be conducted without the data being compromised.