Deloitte.

Credit Card Fraud Detection

August 2023

Agenda

Meet the team	3
Why use AI in the financial industry?	4
Detecting credit card fraud in datasets and AI	5
Data introduction	6
Handling class imbalance	7
Logistic regression with oversampling	8
Delivery methodology and outcomes	9
Model Comparison	10
Conclusion	11

Meet the team

Deloitte AI Practitioners

Jasmine Baker

Risk Financial Advisory Cyber Analyst

Deloitte & Touche LLP

Email: jasbaker@deloitte.com

Experience:

Jasmine is a DevSecOps analyst with a bachelor’s degree in Management Information Systems from Washington State University. She is currently participating in Deloitte’s AI Academy and is passionate about learning new skills.

Shane Reichlin

Risk Financial Advisory Cyber Analyst

Deloitte & Touche LLP

Email: sreichlin@deloitte.com

Experience:

Shane is an analyst with Deloitte & Touche LLP focused in Cyber Identity and PAM. He holds a bachelor’s degree from the University of Washington concentrated in Management Information Systems and is currently participating in the Deloitte AI Academy.

Zomi Yao-Bai

Human Capital Consultant

Deloitte & Touche LLP

Email: zyaobai@deloitte.com

Experience:

Zomi is a visionist with a strong business acumen and an experienced operations consultant, who uses broad prior experience to support clients in improving the efficiency of their value chain.

Nikhil Manimaran

Risk Financial Advisory Cyber Analyst

Deloitte & Touche LLP

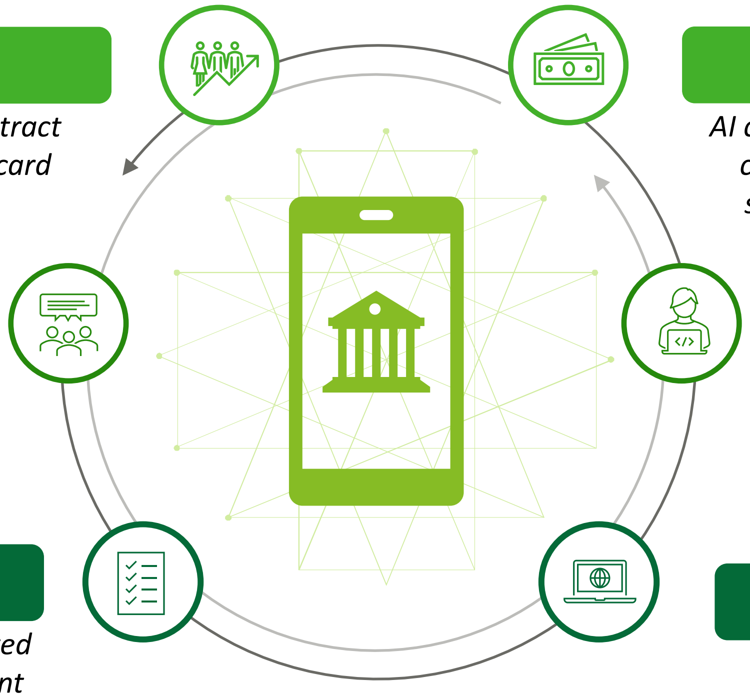
Email: nmanimaran@deloitte.com

Experience:

Nikhil is an advisory analyst and works in the Cyber and Strategic Risk practice. He is a campus hire with a background in Computer Science and AI. He is located in the San Diego Office.

Why use AI in the financial industry?

AI capabilities in the financial industry can improve an organization's reputation, identify credit card anomalies, and improve credit card security.



Reputation

Companies rely heavily on their reputation to attract customers and drive sales. Not detecting credit card fraud accurately or efficiently can permanently damage client relations and consumer trust.

Network Analysis

AI analyzes social networks such as Venmo or Zelle for financial transactions to detect fraud. Network analysis identifies the relationship between individuals and transactions to detect anomalous activities.

Fake Account Creation

To prevent malicious threat actors such as automated bots, AI implements biometric verification, document verification, and validation of personal information techniques to authenticate users.

Card Fraud

AI can detect unauthorized or fraudulent use of credit cards by analyzing transaction data and identifying suspicious activity like usually large transactions or purchases from unusual locations.

Account Takeover (ATO)

Account Takeover (ATO) occurs when a malicious actor steals login credentials for unauthorized access to a victim's account. AI can detect ATO attempts by identifying multiple failed logins. AI can be used to implement multi-factor authentication to mitigate ATO.

Document Forgery

AI can detect document forgery fraud by analyzing digital or physical characteristics of a document such as font, spacing, alignment, and metadata of the document like creation date, location, etc.

DETECTING FRAUD…

In December 2022, the Nilson Report, which monitors the payments industry, released a forecast indicating that U.S. **losses from card fraud** will total **$165.1 billion** over the next 10 years, plaguing **every age group in every state**.

Detecting credit card fraud in datasets and AI

Detecting credit card fraud using AI capabilities can be challenging and AI capabilities are not completely adopted by the finance industry due credit card dataset challenges and modeling challenges.

Challenges

Quantity of Data

There is a large amount of credit card data being processed each day and it can be difficult for a model to keep pace with the amount of data

Class Imbalance

Credit card data contains a class imbalance, often credit card transactions are authentic causing card data to have less fraudulent data points, this creates a data imbalance.

Data Privacy

The data is not always public or available, most credit card data is private and typically must comply with the Payment Card Industry Data Security Standard (PCI DSS).

Malicious Actors

Malicious threat actors can use adaptive techniques against the model as seen with tactics such as skimming.

Opportunities

Dealing with imbalances

Imbalance can be dealt with by resampling the dataset and properly using a random forest model, decision tree model, or a XGBoost model. For our specific example, we utilized SMOTE which is an oversampling technique

Efficient

The model used must be simple and fast enough to detect the anomaly and classify it as a fraudulent transaction as quickly as possible.

Understandable

Use a simple model that is interpretable so that when and if a scammer were to adapt to the model, then we can have a new model up and running to deploy

Data introduction

AI capabilities in the financial industry can improve an organization's reputation, identify credit card anomalies, and improve credit card security.

Dataset

The dataset we used for our model was Credit Card Fraud Detection from Kaggle.

Context

The data set contains credit card transactions made by cardholders in Europe in 2013.

Data

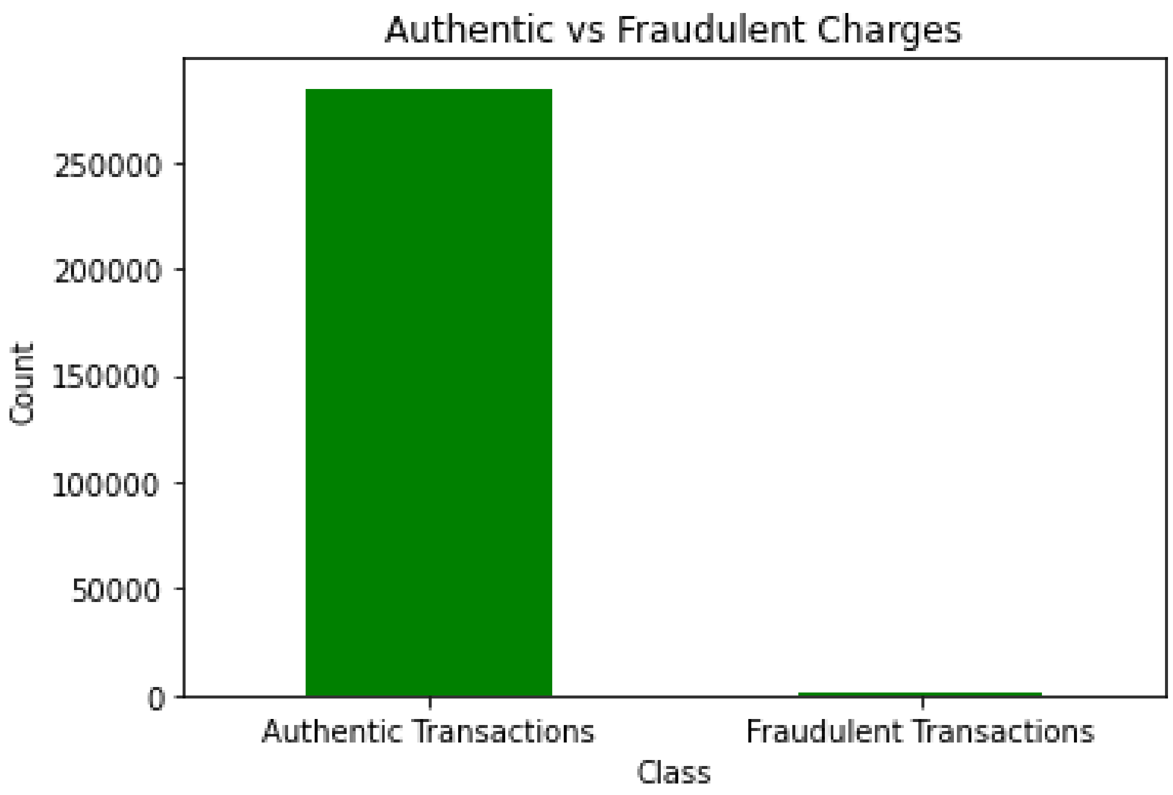
The data set includes the target variable fraud, time, amount, and feature variables V1-V28 which is data specific to the transaction however, due to the sensitivity of the data has been labeled as such.

Content

There are 284,807 transactions in the data set and 492 of these transactions are fraudulent (0.172%).

Correlations

From data analysis and visualizations, we noticed that certain feature variables were more significant for fraud then others, specifically V14 and V17.



As we can see in the graph above, most of the data points in this dataset are for authentic transactions and there is a very small amount of data points to indicate fraudulent transactions, this causes a class imbalance within our dataset.

Working with imbalanced data

Fraudulent credit card transactions are quite rare relative to valid transactions. This introduces additional layers of complexity that must be considered to achieve the best possible results

Even if a model failed to detect a single instance of fraud in our dataset, it could still be **over 99.8% accurate**.

Correcting data imbalance:

- Undersampling
- Oversampling
- Synthetic Oversampling (SMOTE)

Measuring performance:

Precision

- What proportion of our fraud predictions are correct?

Recall

- What proportion of fraudulent transactions are we able to detect?

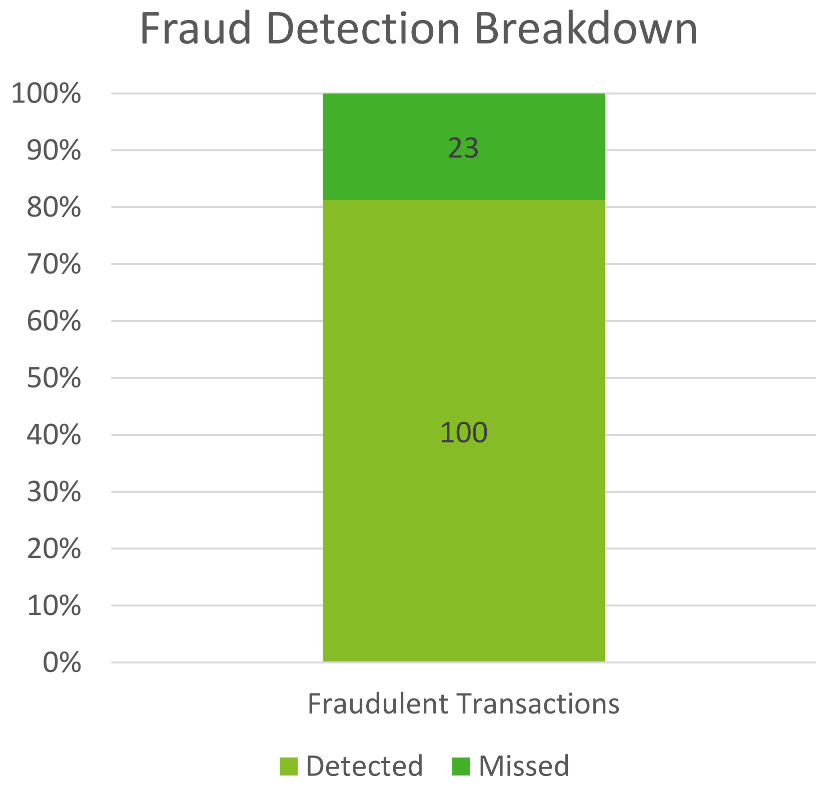
F1 Score

- How does our model perform overall?
- Suitable for comparing results between models

Logistic regression with oversampling

The efficacy of our data preparation is demonstrated here in the results of our optimized logistic regression model

Result: Correctly identified **81.3%** of fraudulent transactions among the unaltered test data while incorrectly flagging less than **0.072%** of valid transactions



Summary:
This model estimates the probability that a given transaction is fraudulent or valid, and classifies it accordingly based on a cutoff value

Pros:

- Simple
- Easy to work with and implement
- Efficient
- Well-suited to binary classification

Cons:

- Does not capture non-linear relationships
- Not as powerful as more advanced techniques

Key Metrics:

- Precision – 0.66
- Recall – 0.81
- F1 Score – 0.73

Delivery methodology and outcomes

A more complex approach to handling imbalances...

Strategic Focus on Weighting Classes & Changing the Metrics

Class Weight or Loss Function Application

ADVISE

- Reprocessing the entire transactions after building the model?
- Class Weight or Loss Function to increase the cost of the failing minority class

Performance Metrics Selection

REVIEW

- Forget the Accuracy Metric
- Classification Report & Confusion Matrix

Goal in Metric Selection

OPERATE

- Optimize Performance on the imbalance production
- Recall & Precision
- Confusion Matrix

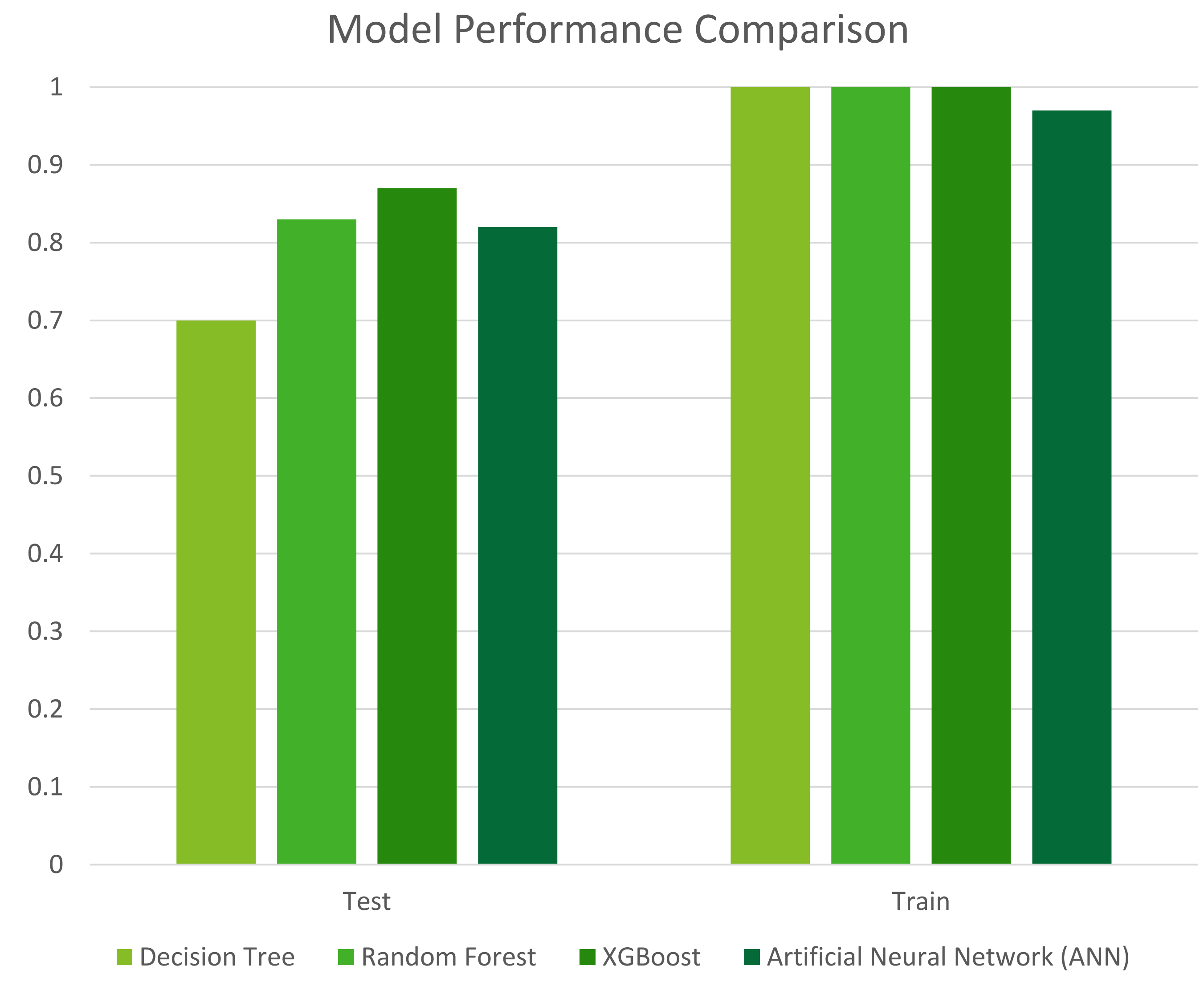
Models Performance Evaluation

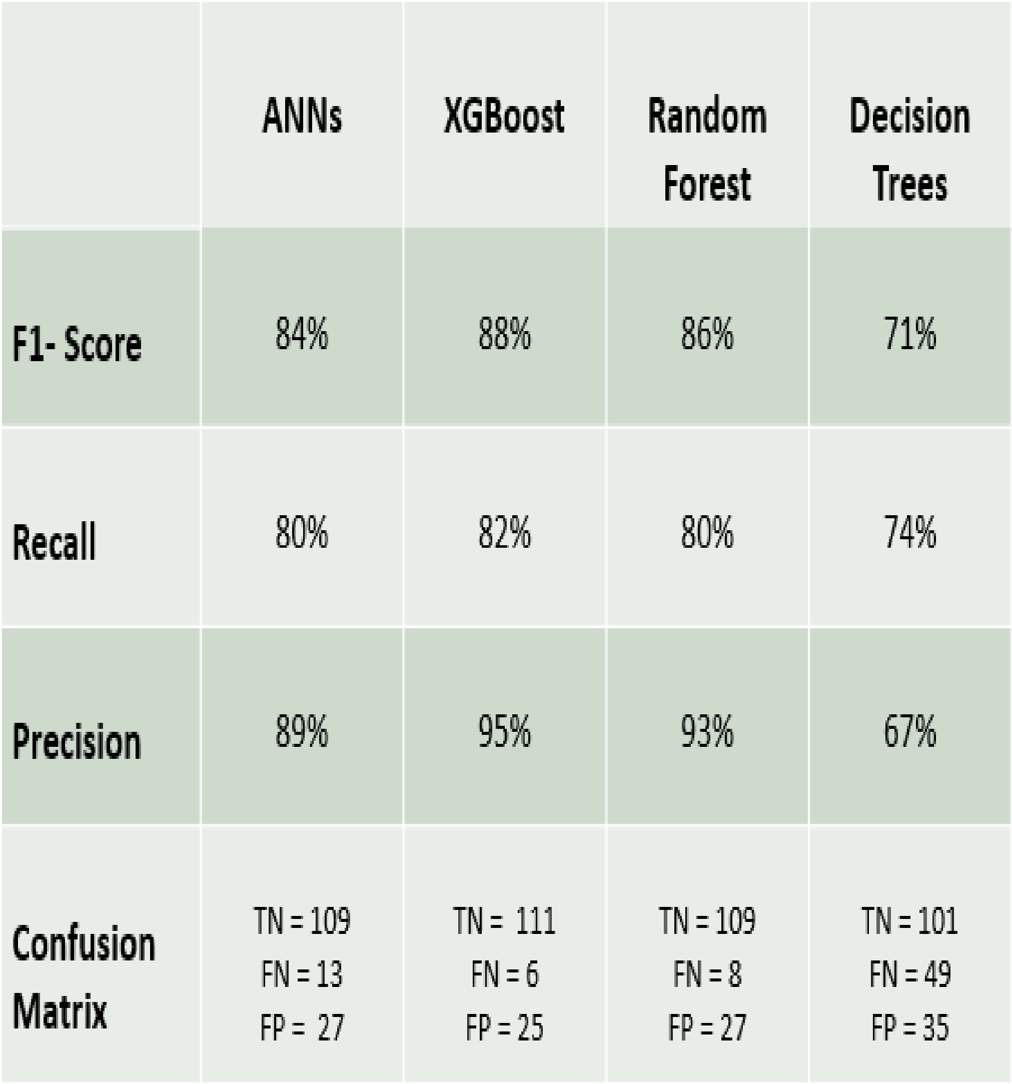
EVALUATE

- Result-driven Decision
- Classifiers results: ANNs, XGBoost, Random Forest, Decision Trees

Model Comparison

We performed a Decision Tree model, Random Forest model, XGBoost model, and Artificial Neural Network (ANN) and found that the **XGBoost model performed the best.**





	ANNs	XGBoost	Random Forest	Decision Trees
F1- Score	84%	88%	86%	71%
Recall	80%	82%	80%	74%
Precision	89%	95%	93%	67%

Confusion Matrix	TN = 109
	FN = 13
	FP = 27
		TN = 111
		FN = 6
		FP = 25
			TN = 109
			FN = 8
			FP = 27
				TN = 101
				FN = 49
				FP = 35

Conclusion

Our Perspective on immediate / future recommendations

❖ Goal:

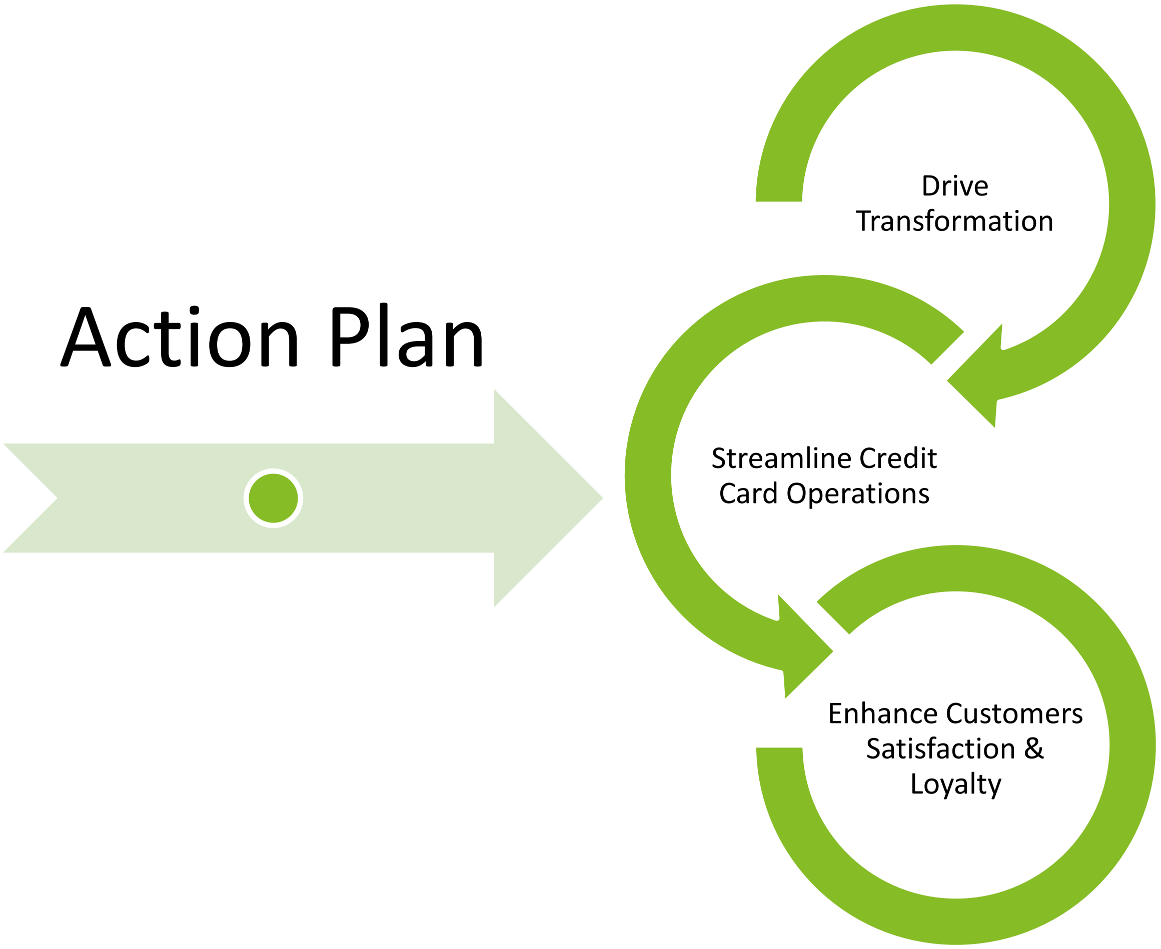
- To detect patterns that correctly show a transaction as fraud

❖ Approach:

- Noticed the number of observations belonging to one class was significantly lower than those belonging to the other classes
- Strategically focused on historical information marked as fraud to achieve an optimization-level class balance
- Selected key performance indicators, compared our models based on them and recommended the model that works best in production.

❖ Recommendation:

- XGBoost corrected the weighting system by placing more weight on those cases which were incorrectly classified in the last transactions
- Captured 95% of all fraudulent transactions , missing only 6 , at the cost of flagging 25 legitimate ones



Action Plan

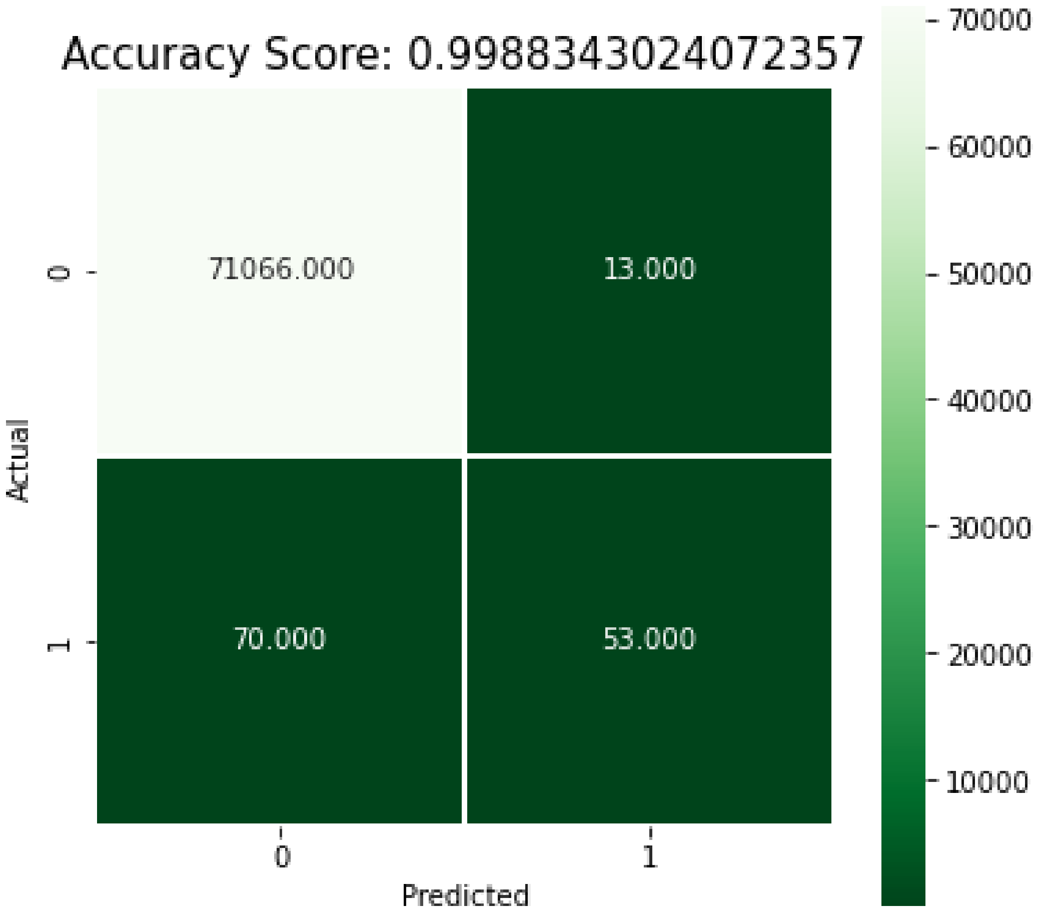
Drive Transformation

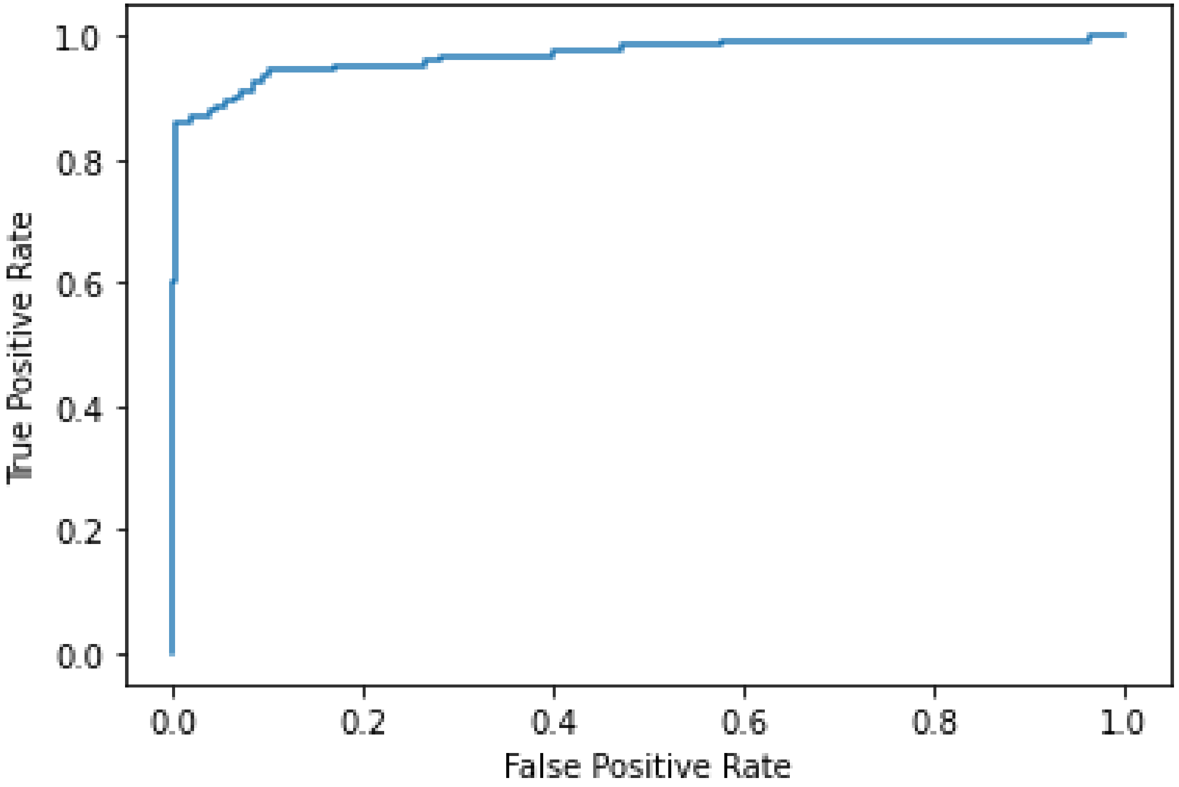
Streamline Credit Card Operations

Enhance Customers Satisfaction & Loyalty

Thank you! Any questions?

Baseline Logistic Regression with unmodified training data





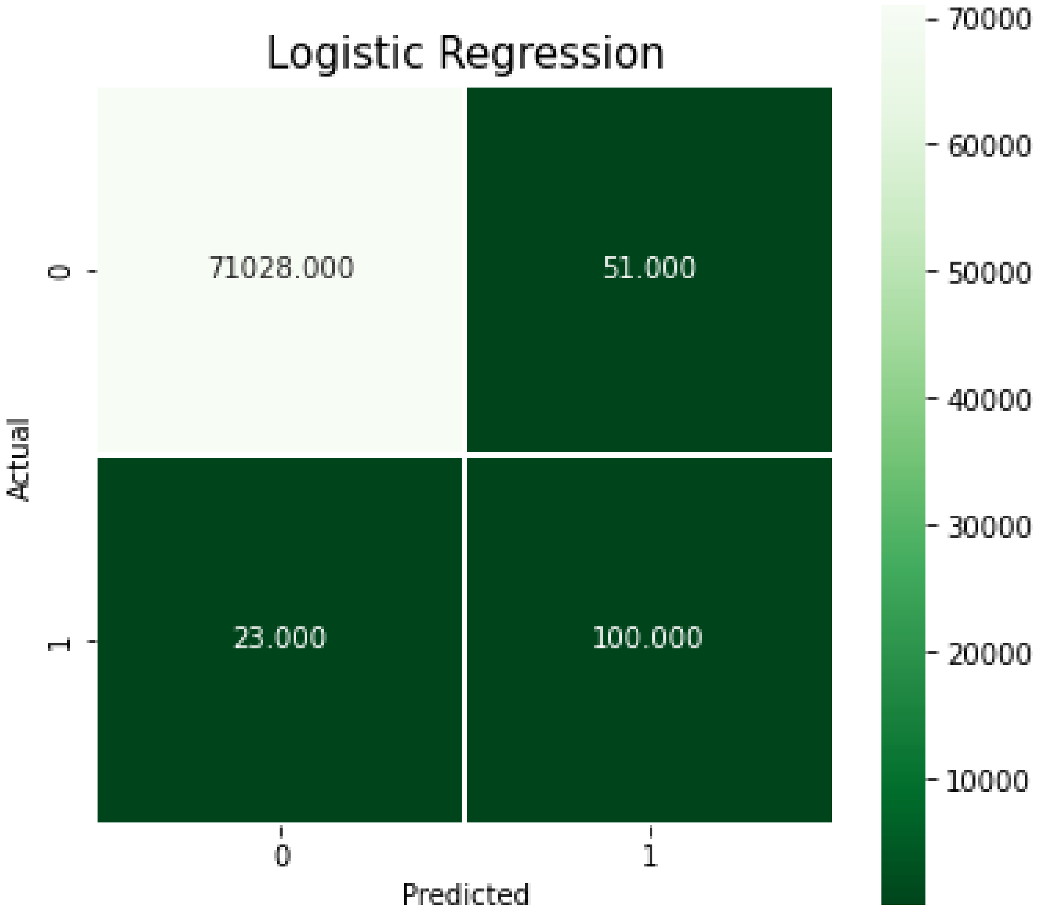
Precision: 0.80

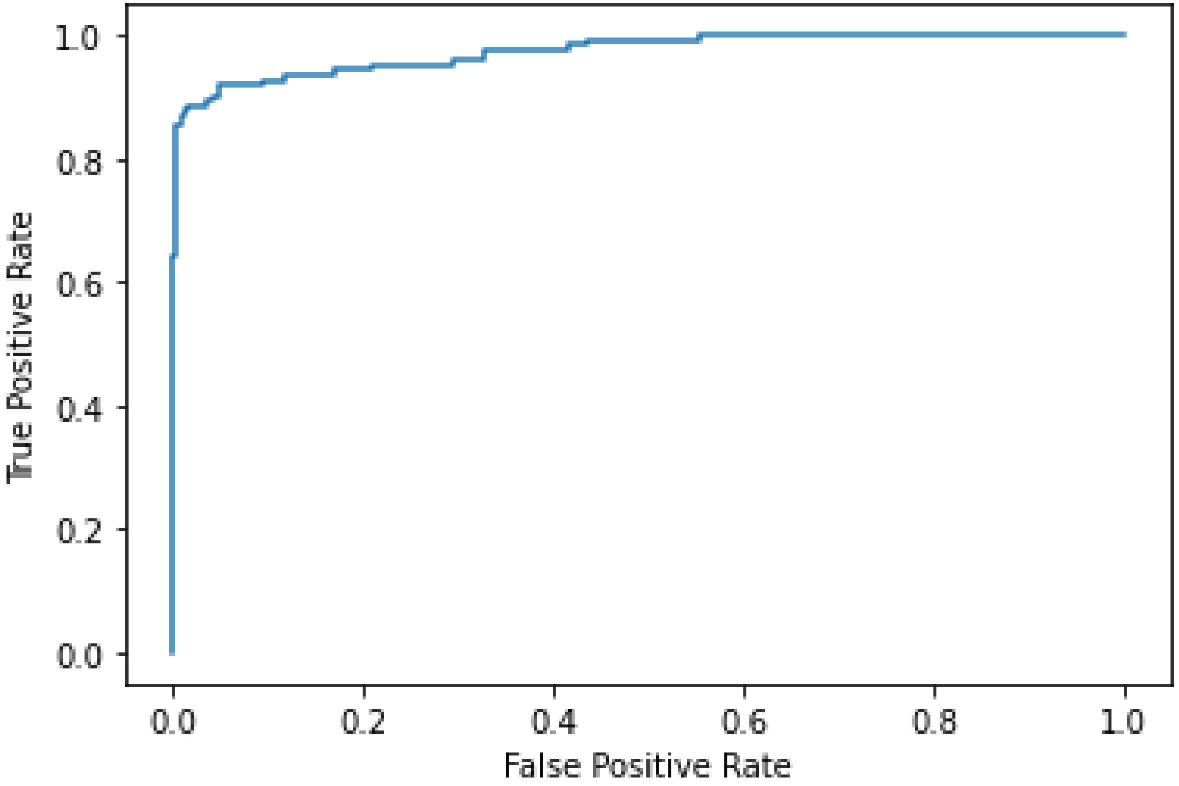
Recall: 0.43

F1 Score: 0.56

AUC: 0.969

Optimized Logistic Regression with Oversampled training data





Precision: 0.66

Recall: 0.81

F1 Score: 0.73

AUC: 0.974