# Prediction of Credit Card Fraud

# Find Default

# AGENDA

- Problem Statement
- Background
- Key findings
- Model Result
- Recommendations
- Appendix:
  - PROBLEM SOLVING METHODOLOGY

# Problem Statement

A credit card is one of the most used financial products to make online purchases and payments. Though the Credit cards can be a convenient way to manage your finances, they can also be risky. Credit card fraud is the unauthorized use of someone else's credit card or credit card information to make purchases or withdraw cash.

It is important that credit card companies are able to recognize fraudulent credit card transactions so that customers are not charged for items that they did not purchase.

The dataset contains transactions made by credit cards in September 2013 by European cardholders. This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) account for 0.172% of all transactions.

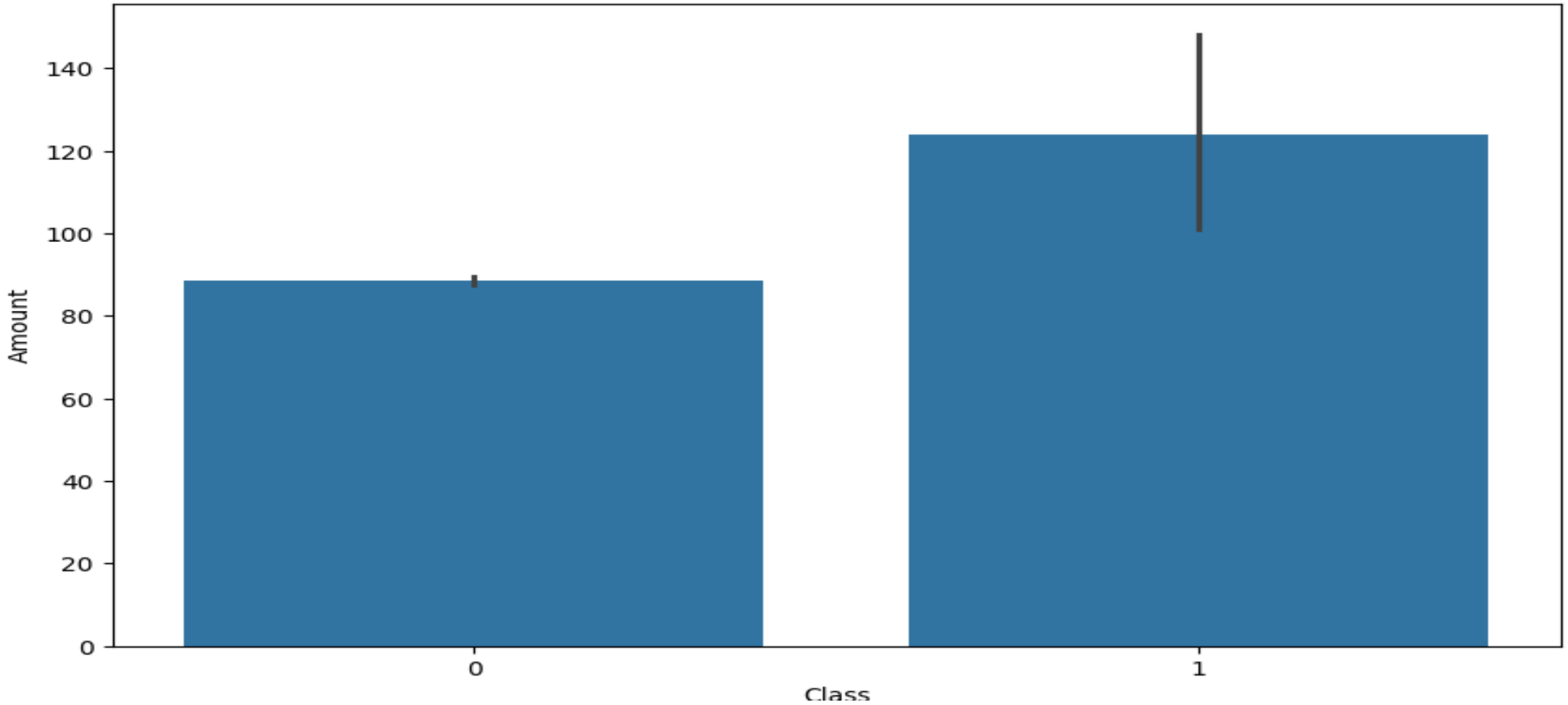
We have to build a classification model to predict whether a transaction is fraudulent or not.

# BACKGROUND

- Fraudsters steal credit card information using skimmers in ATM/POS terminals and make unauthorized transactions.
- The FTC received 416,582 reports from people who said their information was misused with an existing credit card or when applying for a new credit card.
- All cardholders pay for credit card fraud losses.
  - Victims spend time and money to repair the damage.
  - Credit card issuers charge higher fees and interest rates to cover their losses.
  - Loss of customers to the bank.

# KEY FINDINGS

## Amount Vs Class




- It shows that the **class having '1' have more number of fraud amount than other class**.

# MODEL RESULTS

| | model_name | Accuracy Score | Precision Score | Recall Score | AUC Score | f1 Score |
|---|---|---|---|---|---|---|
| 0 | initial_model | 0.978277 | 0.054894 | 0.848 | 0.913234 | 0.103113 |
| 1 | tuned_model | 0.988997 | 0.100691 | 0.816 | 0.902626 | 0.179262 |

- The model has good precision and recall value compared to initial models. So, this model will be good fit in the prediction.

Note: Precision and recall need to be only evaluated on the minor class that is Fraud (1) in our case.

# RECOMMENDATION

- By default all the transactions detected as fraudulent by the model need to be blocked and a second layer of authentication needs to be added. Doing this prevents 95% of the fraudulent transactions from happening.

# APPENDIX - PROBLEM SOLVING METHODOLOGY

**Problem Solving Methodology**

- The approach for this project has been designed to follow the **CRISP DM Framework.** The various stages of the framework are represented below in a sequential flow: