Maayan Hagbi Viktor Kitanov  
Steigerweg 7 Wylerringstrasse 39

3006 Bern 3014 Bern

[Maayan-hagbi@outlook.com](mailto:Maayan-hagbi@outlook.com) viktor.kitanov@hotmail.ch

Final Data Science Project

*Confidential*

Friendly Fraud Detection Model for Enhancing Security in Payment Service Provider Transactions

Final Report

07/15/2024

Abstract

The threat of fraud, particularly in the form of friendly fraud, also known as chargebacks, is a pressing concern for online businesses. Despite its seemingly harmless name, friendly fraud occurs when the person who make the purchase, often the original credit card cardholder, falsely claims a transaction as fraudulent in order to avoid payment. Addressing this challenge effectively is significant challenge for many businesses where often the solution is to apply strict fraud prevention rules on an entire banks or even regions. According to a 2022 sift report, in 2022 online businesses experienced a 35% increase in dispute rates with the average disputed dollar amount increasing close to 16%.

Leveraging data from Fibonatix Ltd, an online payment service provider, our aim is to develop a machine-learning model adept at predicting the likelihood of transactions falling victim to friendly fraud. This initiative is designed to elevate the accuracy and effectiveness in identifying instances of friendly fraud, where seemingly normal customer behavior conceals potentially financially harmful intent.

Contents

[Abstract 2](#_Toc169160186)

[1. Introduction *(content of previously: Project Objectives)* 5](#_Toc169160187)

[2. Data 6](#_Toc169160188)

[2.1. Data Description 6](#_Toc169160189)

[2.2. Metadata 6](#_Toc169160190)

[2.3. Data Quality 6](#_Toc169160191)

[2.4. Data Feature Engineering 6](#_Toc169160192)

[2.5. Data Preprocessing and Cleaning 7](#_Toc169160193)

[2.6. Data Model *(previous text)* 7](#_Toc169160194)

[2.7. Data Flow *(previous text)* 8](#_Toc169160195)

[2.7.1. Unsupervised framework 8](#_Toc169160196)

[2.7.2. Supervised framework 8](#_Toc169160197)

[3. Machine Learning Modelling 9](#_Toc169160198)

[3.1. Tools and Technologies 9](#_Toc169160199)

[3.2. Data Splitting 9](#_Toc169160200)

[3.2.1. Train, Test, and Validation Split 9](#_Toc169160201)

[3.2.2. Timestamp Dependency in Splitting 9](#_Toc169160202)

[3.3. Data Standardization & Dimensionality Reduction 9](#_Toc169160203)

[3.3.1. Application of Robust Scaler 9](#_Toc169160204)

[3.3.2. Principal Component Analysis (PCA) 9](#_Toc169160205)

[3.4. Model Training and Hyperparameter Tuning 10](#_Toc169160206)

[3.4.1. Logistic Regression 10](#_Toc169160207)

[3.4.2. Random Forest 10](#_Toc169160208)

[3.4.3. Neural Network 10](#_Toc169160209)

[3.5. Hyperparameter Optimization 10](#_Toc169160210)

[3.5.1. Comparison of Models 10](#_Toc169160211)

[3.5.2. Best Hyperparameters Selection 10](#_Toc169160212)

[4. Results and Evaluation 10](#_Toc169160213)

[4.1. Evaluation Metrics 10](#_Toc169160214)

[4.2. Model Performance on Limited Dataset 10](#_Toc169160215)

[4.2.1. Full Dataset 11](#_Toc169160216)

[4.2.2. Dataset without Dummies and Coordinates 11](#_Toc169160217)

[4.2.3. Dataset without Profiles 11](#_Toc169160218)

[4.3. Comparison of Model Results 11](#_Toc169160219)

[4.4. Interpretation of Results 11](#_Toc169160220)

[5. Conclusions 12](#_Toc169160221)

[Sources 13](#_Toc169160222)

1. Introduction *(content of previously: Project Objectives)*

Fibonatix Ltd functions as a payment service provider (PSP), offering credit card processing services to a wide array of online businesses spanning across many industries. Notably, within their business operations, friendly fraud emerges as a significant and intricate challenge. The costs associated with friendly fraud extend beyond the direct loss of transactions fees, encompassing operational, processing, reputational costs.

Furthermore, to sustain its operational license, any Payment Service Provider (PSP) must comply with designated chargeback and fraud thresholds set by credit card companies. This underscores the potential harm that chargebacks can inflict on such businesses, emphasizing the imperative need for a robust fraud detection solution.

Our aim is to harness the transactional data supplied by Fibonatix to create a machine learning model that can predict the likelihood of a transaction being reported as fraudulent as close to the time of purchase as possible. This initial step in our initiative is geared towards creating business value by providing the company with sufficient time to investigate potential instances of fraud before they are formally reported. This will essentially give the business time to take the necessary measures to reduce overall risk.

1. Data

*We can start with a Disclaimer of the “Risk” part from your previous paper that we can adjust a bit because it is not about risk assessment, but writing a disclaimer as intro:*

The data provided by Fibonatix is of a sensitive nature, encompassing both customer identifying information (CIDs) and confidential business-related data. In order to mitigate the risk of potential data leaks, a precautionary step is taken during the data extraction stage where all CIDs are anonymized. Strict user rights protocols are implemented, allowing only viewing privileges. Any extraction of data for modeling purposes requires prior approval from Fibonatix, the rightful data owner. Additionally, to fortify Fibonatix's interests, a Non-Disclosure Agreement (NDA) and property rights agreement have been duly executed. These measures collectively ensure the stringent protection and confidentiality of Fibonatix's sensitive business data.

* 1. Data Description

Here we can write that we have access to many different tables in BigQuery and mainly the transactions database. We can then describe the data (columns) in as much detail as we are allowed to (with plots proportion of fraud transactions and so on). (maybe even explain the query briefly – just what we are taking out and not explain the code)

* 1. Metadata

Description of the data sources, data collection methods, and the structure of the dataset, including variable definitions and types

* 1. Data Quality

Here we can write how many transactions we initially have and how many rows we can use for our model/calculations due to missing values or other issues like duplicates.

* 1. Data Feature Engineering

Here we can describe the profiles that we created and the one-hot encoded categories that we defined.

* 1. Data Preprocessing and Cleaning

After describing the data in the beginning we can talk about the data cleansing and merging that we are doing before balancing the data sets. Here we can already mention, that we are conducting three different kinds of tests (full dataset, w/o dummies & coordinates and w/o profiles).

* 1. Data Model *(previous text)*

At its core, the model is designed to assess the likelihood of a transaction falling into one of two categories: potentially fraudulent or not fraudulent. We intend to conduct two distinct operations within this model.

Supervised learning framework:

While the original dataset is inherently supervised, our initial strategy revolves around treating the data as unsupervised. The aim is to unveil distinctive clusters that differentiate between fraudulent and genuine transactions.

To achieve this, we intend to employ Principal Component Analysis (PCA) for pattern detection and K-means for cluster identification. This unconventional approach to an initially supervised dataset seeks to reveal unique patterns and structures that might not be immediately evident within traditional supervised frameworks.

Supervised learning framework:

In the subsequent supervised learning framework, our focus shifts to employing advanced modeling techniques such as Logistic Linear Regression, Random Forest, or Neural Networks.

The objective is to enhance our ability to predict fraudulent transactions within the dataset. This approach leverages the labeled data to train models capable of capturing intricate relationships and patterns, contributing to a more accurate and targeted identification of fraudulent activities.

* 1. Data Flow *(previous text)*
     1. Unsupervised framework
     2. Supervised framework

1. Machine Learning Modelling
   1. Tools and Technologies

*Previous text: Both the analysis and modeling phases of this project will be conducted using the Anaconda Distribution for Python, specifically utilizing Jupyter Notebook and Google Collab for specific tasks as well as a Git repository for version control. The following libraries will be essential for various aspects of the project:*

* *Pandas: Used for data analysis and management.*
* *NumPy: Applied for analysis, data cleansing, and preparation for machine learning models.*
* *Matplotlib: Utilized for data visualization.*
* *SciPy: Employed for statistical analysis.*
* *Scikit-learn: Utilized for machine learning modeling and performance evaluations.*
* *TensorFlow: Applied for machine learning functionalities.*
* *Seaborn: Used for data visualization enhancement.*
* *Time: Employed for performance evaluation metrics.*
  1. Data Splitting
     1. Train, Test, and Validation Split

Explanation of how the dataset is split into training, validation, and test sets,…

* + 1. Timestamp Dependency in Splitting

…with a focus on maintaining temporal order (Mentioning the importance of preserving the sequence of data based on timestamps during splitting).

* 1. Data Standardization & Dimensionality Reduction
     1. Application of Robust Scaler

Explanation of the standardization techniques used to normalize the data before modelling (Description of how the robust scaler is applied to handle outliers and scale the data.).

* + 1. Principal Component Analysis (PCA)

Details on the use of PCA to reduce the number of features while retaining as much variance as possible (Explanation of the PCA process and its impact on the dataset.).

* 1. Model Training and Hyperparameter Tuning

Overview of the machine learning models used and the process of tuning their hyperparameters.

* + 1. Logistic Regression

Description of the hyperparameters of the logistic regression model and its application.

* + 1. Random Forest

Details of the hyperparameters of the random forest model and its use in the project.

* + 1. Neural Network

Explanation of the hyperparameters and of the neural network architecture and training process.

* 1. Hyperparameter Optimization
     1. Comparison of Models

Discussion that we are calculating and comparing combinations of hyperparameters to find the optimal combination based on model performance metrics.

* + 1. Best Hyperparameters Selection

Elaboration that we are only running the best performing model (best dataset and best hyperparameters obtained from the tuning process) using the unfiltered dataset.

1. Results and Evaluation
   1. Evaluation Metrics

Introduction to the metrics used to evaluate model performance (Accuracy, Precision, Recall, and F1-Score).

* 1. Model Performance on Limited Dataset

Presentation of the model performance (results of the evaluation metrics of the different hyperparameters combinations) on different versions of the dataset.

* + 1. Full Dataset

After identifying the best performing model with the best hyperparameters combination, keep this as the best performing combination for 4.3

* + 1. Dataset without Dummies and Coordinates

After identifying the best performing model with the best hyperparameters combination, keep this as the best performing combination for 4.3

* + 1. Dataset without Profiles

After identifying the best performing model with the best hyperparameters combination, keep this as the best performing combination for 4.3

* 1. Comparison of Model Results

Comparison of the performance of the three best performing models above. Decision on the best model for which we will do the testing on the unlimited dataset.

* 1. Interpretation of Results

Discussion and interpretation of the results of the overall best performing model, including insights and implications for the problem statement and objectives.

1. Conclusions

Implementing machine learning models in an e-commerce setting to mitigate various forms of fraudulent activities, including friendly fraud, is a widespread practice in many businesses. Several Software as a Service (SaaS) providers specialize in precisely addressing this challenge. However, industry experts argue that the concept of a one-size-fits-all solution is fundamentally flawed. Each business possesses distinct requirements, making off-the-shelf fraud prevention software often suboptimal as they fail to account for the unique characteristics and needs of individual businesses.

This underscores the potential for us to develop a tailored fraud detection solution specific to the needs of Fibonatix, generating significant business value through effective fraud mitigation.

Sources

1. <https://pages.sift.com/rs/526-PCC-974/images/Report_2022_Q4_Digital-Trust-Safety-Index.pdf>