Strengthening Fraud Detection, Building a Powerful Model for ASB's Digital Future

The data used for this project were synthetically generated

BUSINFO 740 - 2024 Quarter 3
Master of Business Analytics

GROUP 19 :
Deepanjali Kumar - dkmu128
Guoer Li - gli182
Nathan Jing - pjin128
Nurroh Habibah - nhab751

THE UNIVERSITY OF AUCKLAND NEW ZEALAND

ASB

Background

- **ASB,** a bank in New Zealand, is increasingly **challenged by the need to detect fraudulent transactions** as digital banking grows accurately
- The **current** fraud detection **system has room for improvement**, which may result in financial losses and a decline in customer trust
- This analysis **aims to help** ASB **develop a robust model** to **accurately detect fraudulent transactions** and **provide actionable insights** for improving fraud detection

Dataset Overview

500,000 observations

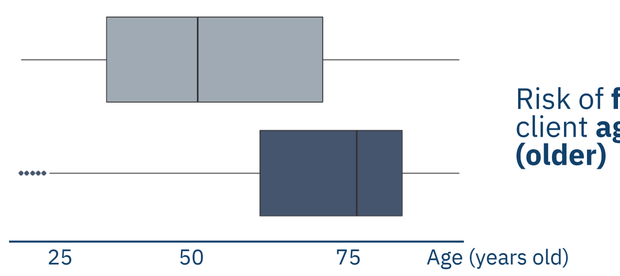
13 variables

May - July 2024

Fraud **Percentage**: **2%**

Fraudulent **Agents**: **34%** ATM · **29%** Mobile · **24%** Desktop · **13%** Others

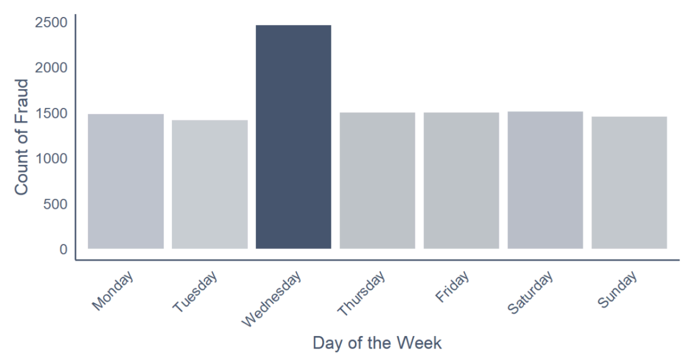
Client's **Age**



Risk of **fraud increases** as client **age increases (older)**

Transaction Type: **34%** Transfer · **34%** Withdrawal · **32%** Purchase

Fraudulent - Transaction **Day**



median **$ 100**

Fraudulent - Transaction **Amount**

Assumptions

- The team **acts as in-house consultants** for the bank
- The patterns in the data remain **stationary** over time
- The model is **scalable**
- The model prioritizes **key features**
- **No multicollinearity** between variables
- **Imbalanced data addressed** through model-building steps
- The classification **cut-off set at 0.5**
- **Leakage-free** between training and test sets

Methods

1 - Data preparation

- Data transformation
- Data inspection
- Exploratory Data Analysis (EDA) through statistical analysis *(Chi-square and T-test)* and visualization
- Variable selection :

Fraud label: Age, Transaction amount, Transaction type, Agent category, Transaction day

2 - Pre processing

Make the dataset ready for the machine learning model to learn effectively

Splitting data: 70% train | 30% test

- Overcome the imbalance data
  - normalization
  - handling categorical variable (encoding)
  - upsampling and dummy
- Creating recipe

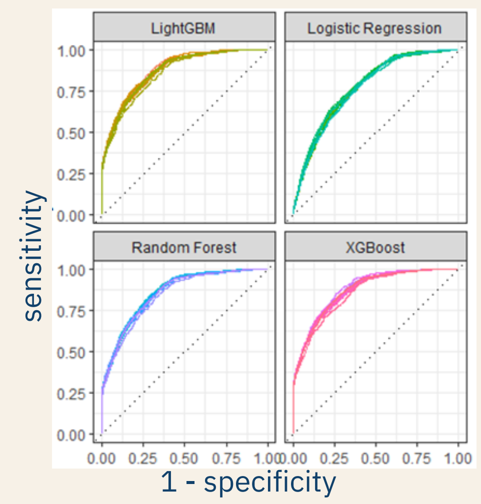
10 K-Fold Cross-Validation

3 - Fitting model to training set

- Define model and workflow
- Fit the model to the folds
- Examine and compare results
- Choose the best model

Accuracy	Sensitivity	PPV	
0.672	0.717	0.048	Logistic Regression
0.747	0.771	0.066	Random Forest
0.761	0.780	0.070	LightGBM
0.760	0.781	0.070	XGBoost

ROC



Focus on model selection by **prioritizing sensitivity (sensitivity)** and **precision (PPV)** to maximize fraud detection while minimizing false positives, ensuring customer financial security and trust without disrupting legitimate transactions[1]

The best model

XGBoost
Extreme Gradient Boosting

4 - Fitting model to testing set

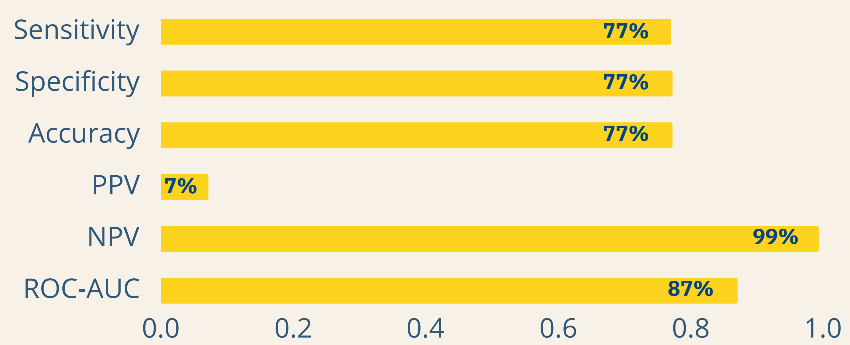
- Apply the chosen model to the test dataset to validate its performance
- Review the final results to assess the model's effectiveness

5 - Interpret result

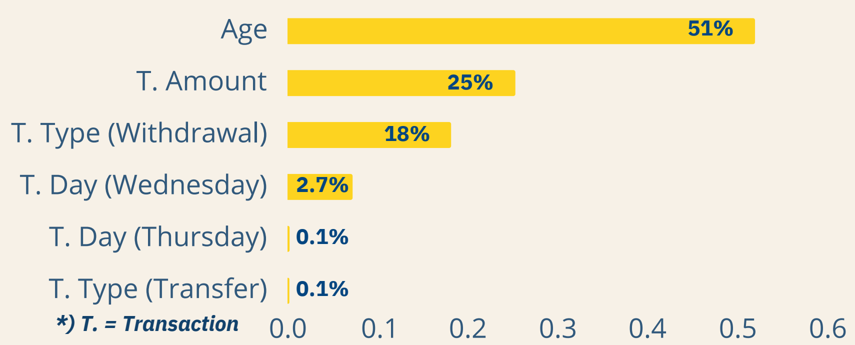
- Provide insights and recommendations based on the model's predictions and performance

Results

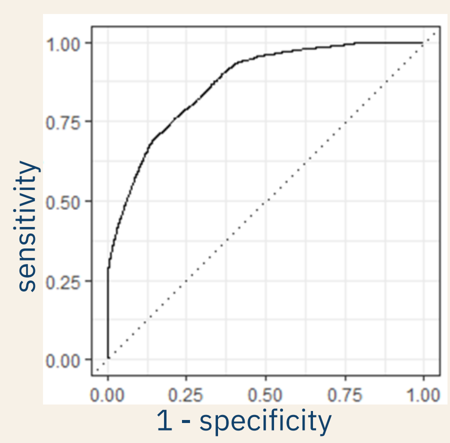
Evaluation Metrics



Prominent Factors Importance



ROC



Confusion Matrix

Prediction \ Actual	Fraud	Non Fraud
Fraud	2,584 (True Positive)	33,376 (False Positive)
Non Fraud	771 (False Negative)	113,269 (True Negative)

Key Insights from the Model

- **Strong performance** and **reliability**
- **Accurately** identified fraudulent and non-fraudulent transactions, **preventing potential financial losses**
- **High** false positives, **but** it gives **opportunity** to **enhance customer trust** and **efficiency**
- **Age** is the **most significant factor** in predicting fraud, followed by **transaction amount** and **transaction type (withdrawal)**, with **other factors having minimal impact**

Definitions of each metric and other statistical terms can be found in the glossary

Conclusion & Recommendation

Two-Tier Fraud Flagging System

Implement a flagging system that **categorizes transactions as lower-risk or higher-risk, triggering automated alerts** for verification accordingly

Lower-risk
- **Infrequent** or **small** transactions <$100
- **Automated alerts** (e.g., SMS, email, or app verification)

Higher-risk
- **Suspicious** or **large** transactions >$500
- **Rigorous verification by call**
- **2-factor authentication**

Strengthen Fraud Management and Customer Security

- Create a **dedicated team** to **review flagged transactions** with **empathetic customer handling**
- Implement **automated reminders** for **security checkups** or **PIN renewal**

Secure Withdrawals and Transfers

- Implement **Extra Verification Layers**
  Introduce **one-time passwords (OTPs)** and **biometric authentication** for added security
- **Set Daily Limits**
  Establish **limits on large withdrawals and transfers** to control transaction volumes

Optional Customer Security Activation

Offer clients a **security delay** for **suspicious transactions** (**30 minutes to 1 hour**) for **customer confirmation** and **additional bank verification**[2]

Glossary

- **Sensitivity:** Measures the ability of the model to correctly identify actual fraud cases
- **Specificity:** Indicates how well the model correctly identifies legitimate transactions
- **Accuracy:** Reflects how often the model's overall predictions are correct
- **Positive Predictive Value (PPV):** Indicates the percentage of transactions flagged as fraud that are actually fraudulent
- **Negative Predictive Value (NPV):** Shows the percentage of legitimate transactions that are correctly identified as non-fraudulent
- **Receiver Operating Characteristic & Area Under the Curve (ROC-AUC):** Represents the effectiveness of the model in discriminating between fraud and non-fraud at various thresholds
- **True Positive:** A correct identification where the model accurately flags a fraudulent transaction
- **True Negative:** A correct identification where the model correctly identifies a legitimate transaction as non-fraudulent
- **False Positive:** The model incorrectly identifies a legitimate transaction as fraudulent
- **False Negative:** The model fails to identify a fraudulent transaction, allowing it to be processed as legitimate

Acknowledgment & References

- The authors acknowledge the invaluable assistance of ChatGPT in brainstorming ideas, debugging code, and refining grammar throughout this project
- We would also like to thank the 704 Course Teaching Team and Aisling Gu from ASB for their valuable advice and guidance in completing this project

[1] Bentivegna, M. (2020). Precision Vs. Recall – Evaluating Model Performance in Credit Card Fraud Detection. *Medium.* https://towardsdatascience.com/precision-vs-recall-evaluating-model-performance-in-credit-card-fraud-detection-bb24958b2723

[2] HSBC Innovation Banking. (2023). *Cut-off times and value dates.* HSBC Innovation Bank Limited. https://www.hsbcinnovationbanking.com/payments-and-fx-cutoff-times