Leveraging Machine Learning Based Fraud Prevention for Customer Experience Optimization

Background

- One of the largest cryptocurrency exchanges is preparing to launch an ethereum-based NFT marketplace which will compete with major players in this space, including OpenSea which has traded over $10 billion in volume in 2021 and $12 billion in volume in Q1 2022
- However, they recently experienced a significant security breach which resulted in the loss of account funds for thousands of customers
- The hackers carried out large-scale phishing campaigns and social engineering attacks that allowed them to access email addresses, passwords, and phone numbers associated with their customer's accounts
- Hackers also exploited a vulnerability in the company's account recovery process allowing them to bypass the company's SMS multifactor authentication (i.e., one-time password) system

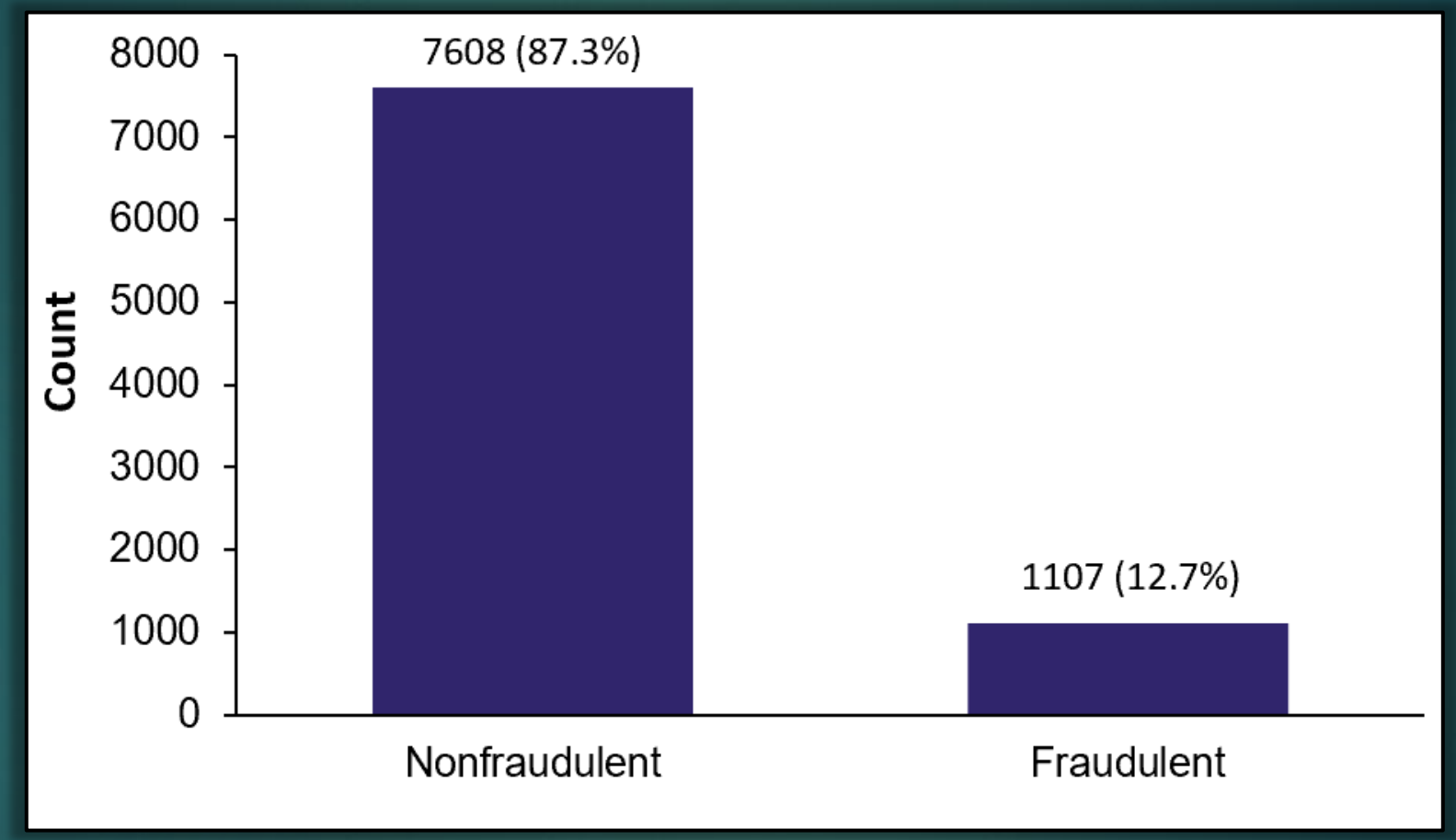
Therefore, despite the growing excitement surrounding the cryptocurrency ecosystem, the occurrence of fraudulent activity may prevent mainstream adoption

Problem Identification

- In order to address the recent security issues encountered by the client, the cryptocurrency exchange has asked customers to take extra steps to ensure the safety of their accounts, including using a more secure method of multifactor authentication (i.e., hardware-based security keys or authenticator applications with time-based one-time passwords)
  - However, the customer experience team acknowledges that this process places the burden of security even more on the customer than previously and there is an understanding that many customers will not take the extra security measures, leaving them vulnerable to future security breaches
  - Likewise, the additional steps needed to buy and trade cryptocurrency and NFTs may detract from the customer experience for those that do decide to adopt the extra security measures

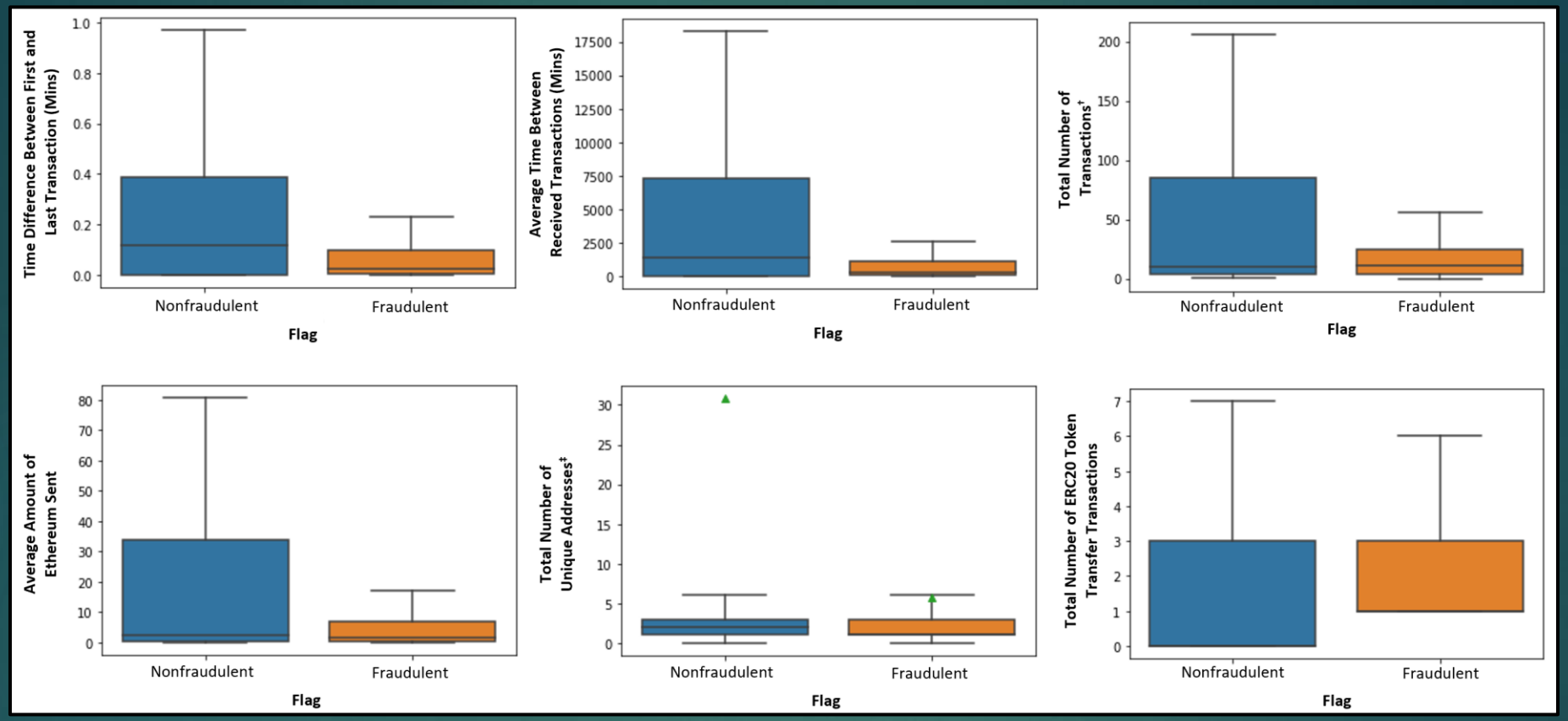
The team understands that utilizing machine learning methods to identify fraudulent accounts owned by bad actors on the ethereum blockchain network would not only improve security but also reduce the burden of security on the customer, resulting in a more positive customer experience

Univariate Distribution of the Target Variable



Of the 8,963 accounts included in the analysis, 7608 (87.3%) were nonfraudulent and 1,107 (12.7%) were fraudulent

Transaction Activity Differences Between Nonfraudulent and Nonfraudulent Accounts



Nonfraudulent accounts tend to have increased transactional activity compared to fraudulent accounts for all features except the total number of ERC20 token transactions

*P < 0.05 for all comparisons.
†Total number of transactions, including contract development transactions.
‡Mean number of unique addresses denoted by green triangle (nonfraudulent: 30.8; fraudulent: 5.7).

Heatmap of Feature Correlation Coefficient Matrix

The correlation between the target and the independent variables are as follows:

(1) Average time between received transactions (score: -0.1)

(2) Time difference between the first and last transaction on the account (score: -0.18)

(3) Total number of unique addresses accounting for all outward-bound transactions (score: -0.032)

(4) Average amount of ethereum sent (score: -0.033)

(5) Total number of transactions (score: -0.071)

(6) Total number of ERC20 token transfer transactions (score: -0.022)

Avg, average; Txns, transactions.

*Time in minutes

†Total number of transactions, including contract development transactions.

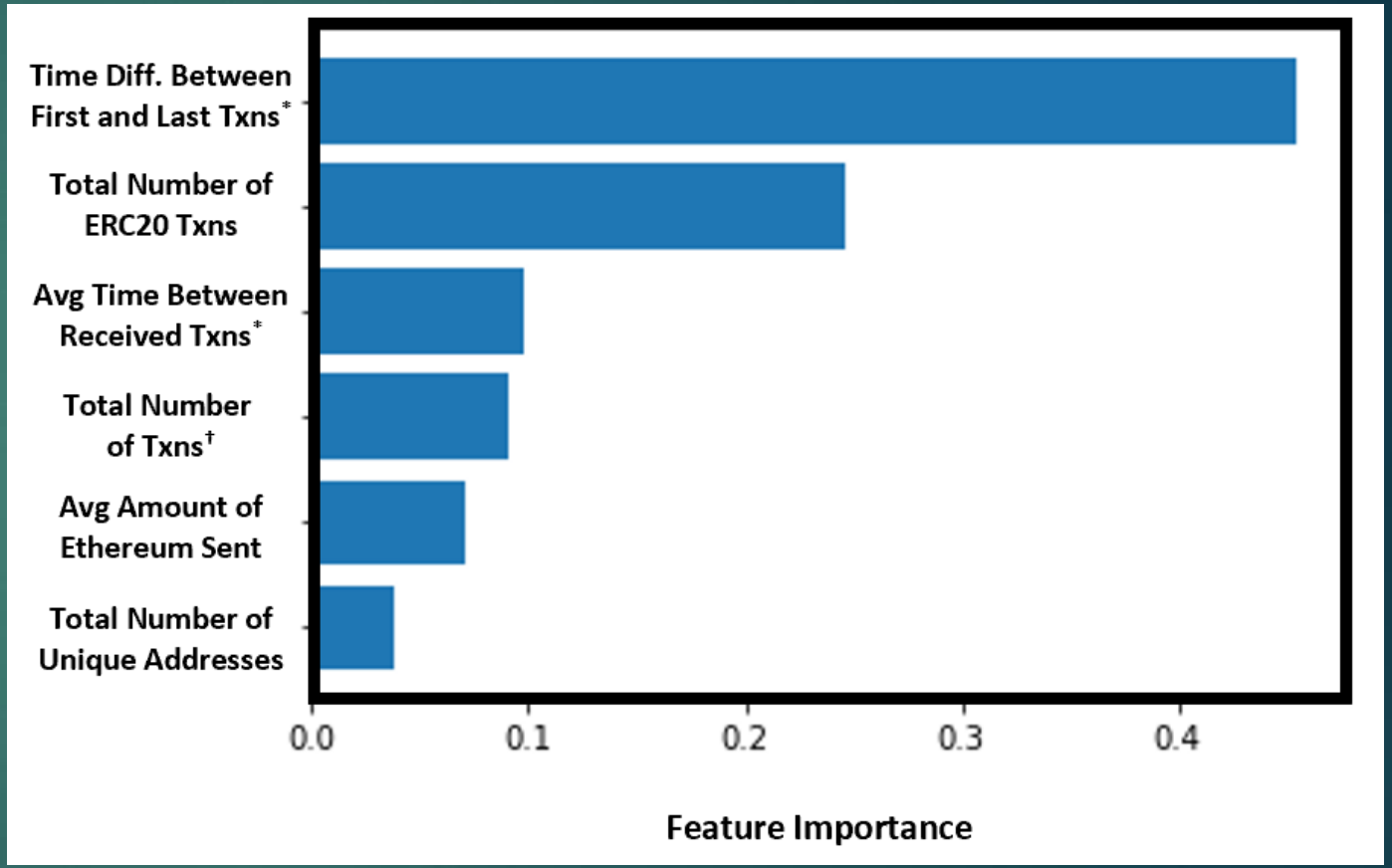
Feature Importance Analysis

Features were ranked by predictive performance. The three most important features include:

(1) The time difference between the first and last transaction on the account

(2) Total number of ERC20 token transfer transactions

(3) Average time between received transactions



Avg, average; Diff, difference; Txns, transactions.
*Time in minutes
†Total number of transactions, including contract development transactions.

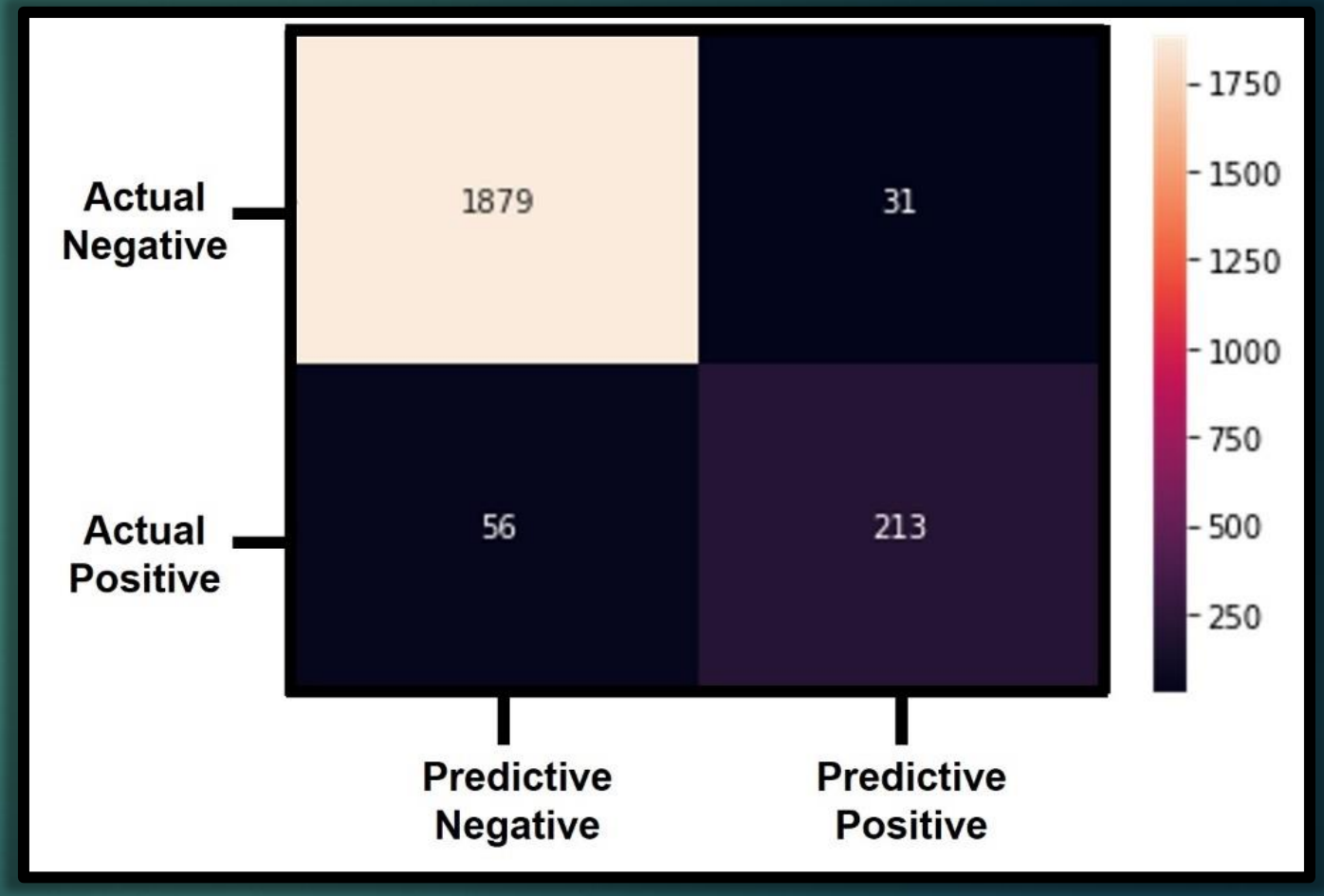
ROC-AUC Based Model Performance Comparison

Classifier	ROC-AUC Score	Hyperparameter Values
Random Forest	0.9853	criterion = entropy, max_depth = 100, max_features = sqrt, n_estimators = 100
Gradient Boosting	0.9852	learning_rate = 0.1, max_depth = 100, max_features = sqrt, n_estimators = 300
K Nearest Neighbor	0.9630	n_neighbors = 20, weights = distance, p = 1
Support Vector Machine	0.9538	C = 1, gamma = 1
Naïve Bayes	0.7442	var_smoothing = 0.1
Logistic Regression	0.7228	max_iter = 250, C = 0.001

ROC AUC, receiver operating characteristic area under curve..

Predictive Performance of Optimized Random Forest Classifier

Prior to thresholding by the false discovery rate, the random forest model resulted in the correct classification of 2092 (96%) accounts with 56 (2.6%) accounts incorrectly classified as nonfraudulent and 31 (1.4%) accounts incorrectly classified as fraudulent



Predictive Performance of Optimized Random Forest Classifier (FDR = 0.02 vs 0.05)

Classifier	Correctly Classified	Incorrectly Classified As Nonfraudulent	Incorrectly Classified as Fraudulent	Precision & Recall
Optimized Random Forest Model	2092 (96%)	56 (2.6%)	31 (1.4%)	0.87 & 0.79
Optimized Random Forest Model (FDR = 0.02)	2098 (96%)	12 (0.5%)	69 (3.2%)	0.94 & 0.74
Optimized Random Forest Model (FDR = 0.05)	2021 (92.7%)	146 (7%)	12 (0.5%)	0.64 & 0.96

FDR, false discovery rate.

Conclusion

- The utilization of a machine learning based fraud detection system would significantly improve the customer experience by shifting the burden of security from the customer to the company
- This will not only improve the customer experience but potentially improve customer acquisition, retention, and overall profitability
- Also, traditional financial institutions are entering the cryptocurrency space at a rapid rate
  - These institutions already have robust security measures in place and do not solely rely on onerous multifactor authentication measures to keep their customers safe
  - As a result, these institutions will quickly become fierce competitors

Therefore, centralized cryptocurrency exchanges will need to adopt more sophisticated security processes to remain competitive

Conclusion (cont.)

- In this analysis, the random forest classifier outperformed the gradient boosting, K nearest neighbor, support vector machine, naïve bayes, and logistic regression classifiers
- Prior to choosing the optimal detection threshold, the client will need to determine if it is more beneficial to select a threshold that would minimize payout due to fraud or improve the customer experience by selecting a threshold that minimizes false positives
- If the client is more concerned with minimizing payout, the optimal detection threshold would be based on a false discovery rate of 5%
- If the client is more concerned with decreasing the number of false positives, the optimal detection threshold would be based on a false discovery rate of 2%

Lastly, as cryptocurrencies and NFTs on other blockchains become more popular (i.e., Tezos, Flow, Solana, Cardano), the fraud prevention strategy may need to evolve based on the data available on other blockchains

Thank You!