Billions are on the line, who are you going to call?

The Fraud Fighters

Identifying Fraud in Mobile Money Transfer Services

INTRODUCTION

Credit card fraud and financial statement fraud have been pervasive in our economy and society for many years. Such fraud has cost companies, consumers and society exorbitant amounts of time and money. For example, two of the largest credit card security breaches to date, TJX in 2007 and Target in 2013, are alone responsible for leaking over 80 million credit card numbers to scammers due to ineffective security of their point of sale systems. Mobile money transfer services (MMTS) are newer types of financial transactions that are currently being deployed in many markets across the world and are widely used for domestic and international remittances. MMTS transactions, like credit cards and financial statements, are highly susceptible to fraud. Fraud detection of MMTS transactions and similar financial services is an important and significant endeavor.

Data mining and modeling techniques have evolved sophisticated probabilistic models to detect credit card and financial statement fraud, and with the emergence of MMTS transaction probabilistic models are now necessarily being developed to detect fraud in MMTS transactions. We studied the predictive models used for credit card and financial statement fraud, as well as those used specifically for MMTS transactions, such as the RadViz visualization technique and Predictive Security Analyser. We then utilized a synthetic data set with a combined three clustering algorithm that is applied dynamically to attempt to detect fraud in MMTS transactions in real time.

CONTRIBUTORS

- Mary Donovan Martello
- Evan Edmunds
- Samarah Lopez
- Ramizuddin Mohammed Shabuddin
- Kurt Stoneburner

Bellevue University
Data Science 500

Less than 1% fraud represents over a billion in losses

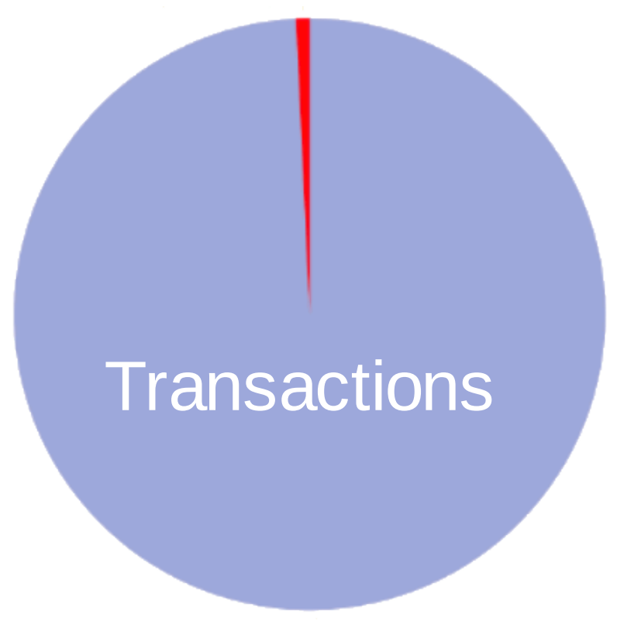
	Transactions	Transactions %	Cash	Cash %
Fraud	1,142	0.11%	1,221,982,240.43	0.74%
Valid	1,047,433	99.89%	165,012,241,622.94	99.26%

WHY IS THIS DATA SCIENCE?

The prevalence of electronic transactions generates an immense digital footprint of consumer purchases. The popularity and ease of use of mobile money transfer services makes them targets for fraud. These attributes also means that there are large, structured data sets containing thousands of user transfers.

Data mining provides a method of finding patterns within a data set that could not be observed otherwise. Patterns found can be further analyzed by a computer through modeling of the data that allows for extrapolations to be drawn from future data points. This final product is then able to provide a solution to a problem in the real world faster and more accurately than a human. The solution created will fulfill a business need that is required to operate effectively in an increasingly technological world.

.11% Fraud is hard to spot



DELIVERABLES

Data and Dynamic Probabilistic Model Solution for Mobile Money Transaction Fraud Detection

Challenges for Fraud Detection in MMTS Transactions

Two significant challenges data scientists must address in detecting fraud in MMTS transactions:

- Data Set Challenges
  - Data set must be extremely large and imbalanced to be properly trained
  - There is a dearth of publicly available financial transaction data
- Time Challenges. To be effective in preventing fraudulent transactions, the predictive model must be used in real time.

Our Solution for Fraud Detection in MMTS Transactions

Our data approach and predictive model addresses the challenges in for models to detect fraud in MMTS transactions.

- Data Approach: Use a PaySim simulated synthetic data set to train and test our model. PaySim is a financial simulator that simulates mobile money transactions based on an original dataset.
- Model for MMTS Transactions: Dynamic Tri-Clustering Algorithm
  - New transaction is tested in the model as the transaction is happening
  - Use of three different unsupervised clustering algorithms simultaneously optimizes accuracy

OBJECTIVES

❑ Research fraud events and statistics to display the damage that can occur to revenue and reputation of an organization and the need for advanced fraud prediction models.

❑ Investigate current fraud monitoring techniques available for various monetary systems (credit card, financial statements, etc.).

❑ Use algorithms and monitoring techniques of other fraud prevention systems to develop a predictive model that monitors mobile money transfer services for potential fraudulent activity.

CONCLUSIONS

Losses from online payment fraud are predicted to more than double by 2023, reaching $48 billion annually. Developing methods to detect mobile money transfer fraud is essential to combat fraud attempts on these transactions. Dynamic modeling techniques are an important component of preventing mobile money transfer fraud as they find patterns within extremely large imbalanced data sets that could not be observed otherwise and help provide a solution in real time (or near real time). Our tri-clustering dynamic predictive model was trained on a large imbalanced synthetic data set and will detect mobile money fraud in real time and will assist in reducing fraud in mobile money transfer services.

LITERATURE

- Novikova E., Kotenko I. (2014) Visual Analytics for Detecting Anomalous Activity in Mobile Money Transfer Services. In: Teufel S., Min T.A., You I., Weippl E. (eds) Availability, Reliability, and Security in Information Systems. CD-ARES 2014. Lecture Notes in Computer Science, vol 8708. Springer, Cham
- MINASTIREANU, E.-A., & MESNITA, G. (2019). An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection. *Informatica Economica*, *23*(1), 5–16. https://doi-org.ezproxy.bellevue.edu/10.12948/issn14531305/23.1.2019.01
- Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of Fraud Detection Techniques: Credit Card. *InternationalJournal of Computer Applications*, 39-44.
- Choi, D., & Lee, K. (218). AnArtificial Intelligence Approach to Financial Fraud Detection under IoTEnvironment: A Survey and Implementation. *Security & Communication Networks*, 1-15.
- EdgarAlonso Lopez-Rojas, E., Elmir, A., & Axelsson, S. (2016). PAYSIM: A FINANCIAL MOBILE MONEY SIMULATOR FOR FRAUD DETECTION. *28th European Modeling and Simulation Symposium2016*, (pp. 1-7). Larnaca.
- Phua, C., Lee, V., & Gayler, R. (2010, Septermber 30). *Computer>Science.* Retrieved from Cornell University: https://arxiv.org/abs/1009.6119

Acknowledgements

- Bellevue University course DSC 500: Intro to Data Science, as well as the library resources.
- John D. Kelleher and Brenden Tierney for their knowledge in *Data Science: The MIT Press Essential Knowledge Series*
- Kaggle.com for providing an artificial dataset of mobile money transfers from their simulator, PaySim
- KDNuggets.com, towardsdatascience.com, and neowin.net for various knowledge of the data science field.