Parameter Selection for Friendly Fraud Detection in eCommerce

UDK 004.85:336.717

Dmytro Masiuk

Taras Shevchenko National University of Kyiv, masiukdmitry96@gmail.com

Friendly fraud has become one of the most significant challenges in modern eCommerce systems. Unlike traditional payment fraud, also called “true fraud”, friendly fraud occurs when legitimate customers dispute valid transactions through chargebacks, often claiming unauthorized usage. It has become increasingly simpler for fraudseter to commit fraud, as they can do so in a matter of clicks. Alongside this growth, merchants face increasing financial losses related to chargebacks and payment disputes. According to research in fraud analytics and financial machine learning, modern detection systems increasingly rely on intelligent parameter selection and behavioral analysis techniques to distinguish suspicious behavior from legitimate customer activity [1][3]. This report analyzes the importance of parameter selection in friendly fraud detection for increasing success metrics.

Friendly fraud is particularly difficult to detect because transactions are usually performed using valid customer credentials and legitimate payment instruments. Unlike stolen card fraud, friendly fraud often resembles normal customer behavior during the authorization stage. Fraud detection systems must therefore rely on subtle behavioral and transactional anomalies rather than obvious indicators of compromise [4].

The quality of such systems heavily depends on how good is selection of informative parameters capable of distinguishing fraudulent disputes from legitimate customer actions. Poor parameter selection may result in high false-positive rates, low precision-recall and thus high chargeback rates which lead to financial loss. Parameter selection represents one of the most important stages in the construction of intelligent fraud detection systems.

Parameters, also called features, describe measurable transaction characteristics that can be used for classification purposes. Transaction-related parameters describe financial and temporal characteristics of customer activity, such as purchase frequency or transaction amount. Transaction aggregation techniques can significantly improve fraud detection performance by identifying unusual transactional behavior over time [5].

For example, repeated purchases followed by refund requests within short intervals may indicate potentially abusive behavior. Behavioral analytics focuses on identifying deviations from normal user activity patterns. Common behavioral parameters include device and fingerprint consistency, IP address changes and login behaviour.

According to López de Prado, behavioral signals are especially valuable in modern financial machine learning systems because fraudulent activity often cannot be detected through transactional analysis alone [3]. Behavioral inconsistencies may therefore provide stronger predictive indicators than payment data itself, in some cases.

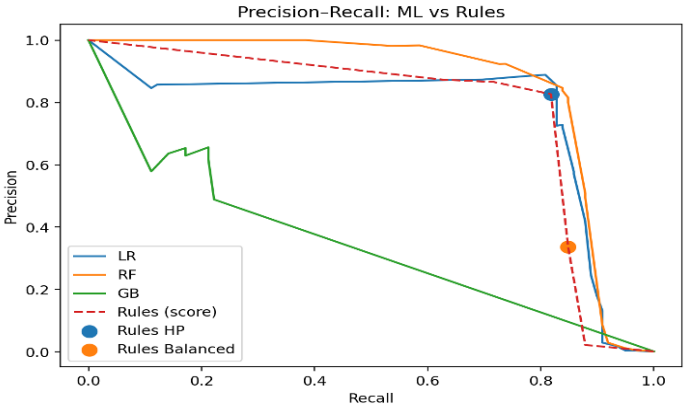

Fig.1. Rule based system with selected features versus untuned Machine Learning models

Historical behavioral information becomes particularly useful when working with highly imbalanced fraud datasets, where fraudulent transactions represent only a very small percentage of total activity [2]. In my previous paper [6] I briefly touched feature selection during an analysis of another topic. In order to determine strongest predictive features, Information Value(IV) was used.

$$IV = \sum_{i=1}^{n} (p_i - q_i) * \frac{p_i + \varepsilon}{q_i + \varepsilon}) \# (1)$$

It can be seen on the graph, that after the feature selection, even though quite simplistic, the rule-based system shows results on par with untuned ML models, while being much faster to run and more explainable. In my future papers I plan to analyze which features are the most important for different fraud types.

1. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50(3), 602–613.
2. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784–3797.
3. López de Prado, M. (2018). Advances in financial machine learning. Wiley.
4. 4. Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review, 34(1), 1–14.
5. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data Mining and Knowledge Discovery, 18(1), 30–55.
6. Gaina, G., & Masiuk, D. Evaluating rule-based vs. machine learning approaches for fraudulent transaction detection