Case Study:

# Boosting confidence in fraud prevention

ZONE3000

**Client:** A mid-sized tech company experiencing significant threats from credit card fraud as it expanded.

## 1. Challenge

The e-commerce platform faced a high rate of fraudulent account activities, resulting insignificant operational and financial challenges:

**Manual investigations:**

A heavy reliance on manual efforts to identify and close fraudulent accounts, consuming substantial resources and time.

**Increased risk:**

The high volume of fraudulent activities posed risks to the platform's accounts with payment processors, threatening operational stability.

**Fraud class imbalance:**

The fraud class constituted a small proportion of overall transactions or accounts, creating significant class imbalances that necessitated advanced techniques to ensure balanced model performance and accurate predictions.

**Chargebacks and transaction cancellations:**

Frequent chargebacks and transaction cancellations led to penalties and jeopardized the platform's compliance with payment processor system thresholds.

## 2. Solution

A multi-layered fraud prevention system was designed to address these challenges, incorporating rule-based methods, Machine Learning (ML) models, and advanced relationship analysis:

**Rule-based detection:**

Hard pattern detection rules were defined as a result of deep data analysis and implemented within the payment processor to identify and block known fraudulent activities.

**Dynamic risk scoring and risk level assessment:**

An ML model as a service was introduced to generate a risk score for user accounts, recalculated with every new activity or transaction. Utilizing account data, user behavior events, history of transactions with scores, and user relations defined. Accounts exceeding a high-risk threshold were automatically blocked. Potential risk accounts were flagged for manual RM review.

**Data pipelines:**

Developed to manage the seamless integration and processing of large-scale transactional and user data efficiently.

**Transaction fraud model and service:**

A deep neural network (DNN) model was developed to analyze transactional data as a time series, leveraging historical user transactions and a set of personal user data, such as location and datetimes of users' logins, user email, etc. High-Risk transactions are automatically blocked. Medium-Risk transactions are flagged for manual review by the Risk Management (RM) team.

**Accounts relationship engine:**

An ML-powered relationship engine was built to map connections between accounts, updating relationships dynamically when new accounts were created or data was modified. This model combined rule-based logic with advanced ML techniques to identify potential collusion or shared fraudulent patterns.

## 3. Technology Used

**API event-based architecture:**

A service-oriented approach where APIs are triggered only when required. These services process the most recent user data shared through event-driven mechanisms from other interconnected systems.

**ML models developed on TensorFlow**

All Machine Learning models were developed using TensorFlow, leveraging its powerful framework for training deep neural networks and large-scale data processing.

**Deep neural networks for time series analysis:**

Applied to analyze transactional data patterns and predict the likelihood of fraud. These models integrate recurrent layers, convolutional layers, and multiple inputs for robust fraud detection.

**Relation engine and risk scoring model:**

The model produces non-homogeneous outputs for more nuanced risk scoring.

**Character vectorization and cosine similarity:**

Used to measure similarities between account profile details.

**Addressing class imbalance:**

Implemented techniques like class weighting, bias adjustments during model training, and artificial upsampling to account for the disproportionately small fraud class, improving prediction reliability and overall model accuracy.

## 4. Result

The implementation of our ML solution led to significant improvements in the company's fraud detection capabilities:

**Fraud model onboarding:**

After the first step of onboarding the transactional ML fraud model, the chargebacks exceeding rate was never reached again, reducing the risk of penalties and account issues with the payment processor.

**Automated transaction blocking:**

By setting thresholds based on model probabilities, fraudulent transactions were automatically blocked with a ~4% false positive rate, covering approximately 30% of all fraud cases.

**Time saved on manual reviews:**

The system significantly reduced the workload for Risk Management specialists by pre-listing potential fraudulent transactions and accounts, streamlining manual review processes. Automated account blocking based on Risk Score alone saved approximately 280 human work hours per month.

**Automated account blocking based on risk score:**

By setting thresholds based on model probabilities, automated account blocking was maintained with a ~3.5% false positive rate, covering approximately 50% of all fraud cases. Total model accuracy was more than 95%.

**Superior performance:**

At the early stage of model development, when compared to AWS Fraud Detector and other market-ready solutions, our Transaction Fraud model and Risk Score models demonstrated significantly superior performance. With an accuracy of ~90% compared to AWS Fraud Detector's 85% on the same validation data samples and the same target metric, our solution also achieved much lower false negative rates, providing a more reliable and efficient approach for fraud detection and risk assessment.

This case study illustrates how **ZONE3000's** strategic approach to implementing a Machine Learning solution effectively addressed the fraud detection challenges faced by the tech company, enabling it to enhance its financial security and protect its reputation in a competitive market.