CASE STUDY

Digital Bank Reduces Fraudulent User Accounts and Transactions

simility

An Innovative Digital Bank Reduces Fraudulent User Accounts and Transactions while Introducing New Features to Manage Money

Overview

A San Francisco based mobile-focused bank targeting millennials grew successfully by differentiating itself with features like no monthly fees, minimum balance requirement, or overdraft fees. Staying true to its millennial appeal, the bank also issued a Visa card targeted at millennials who tend to prefer rewards programs tied to their primary spending account. With an existing base of a few hundred thousand members, the bank embarked on marketing programs to aggressively grow its cardholder base, but had to come up with better analytics to detect fraud and ensure that fraud rate was not growing as new cardholders signed up.

Challenge

Driven by lower thresholds for credit checks, requirements for account origination, and benefits of a rewards programs, millennials traditionally excluded from the banking system and coming of age in the mobile-first era have been adopting this new card. While the acquisition of these customers has been great from a growth standpoint, the risky profile of customers signing up for the card meant the bank had to have a sophisticated fraud detection system in place.

The top challenges of its current fraud prevention tool were:

1. A high fraud rate greater than 1%
2. New rule development and modification of existing rules were not making a significant dent in missed fraud
3. Too many manual reviews were needed to identify fraud patterns
4. Inability to link users to other users via entities like address, phone number and social security number

Solution

The bank compared numerous solutions in the market and chose Simility as its vendor.
It took less than three weeks to customize a model for the bank based on their approved fraud data and historical transaction data.

The key components of the solution that stood out were:

1. Natural language rules UI: Ability to build manual rules based on complex logic in an intuitive manner and ability to test the rules in real-time on historic data.

2. Machine Learning: Simility's Machine Learning algorithms were used to enhance and complement the performance of manual rules. The Machine Learning models provided the bank with insights about transactions and user behavior that were unprecedented and almost impossible to decipher with a manual analysis of data.

3. Graph Analysis: Simility's graph network analyzer allowed the bank to link known bad users and fraud transactions via entities like addresses, social security numbers, phone numbers, and IP addresses, which helped detect major fraud rings.

Insights and Results

An Example of Interesting Insight Provided by Simility:

Average Fraud Rate across all transactions was less than 2%, but for all transactions that met the following criteria the fraud rate was less than 40%:

- AVS checks per user is NULL
- Number of distinct transaction events is between 5 and 15
- Transaction declines per user less than 8.

Machine Learning models were able to provide rule development insights based on statistical correlations that would have been difficult to come by using human intuition or analysis.

The Results Post-Simility Deployment:

- Simility was able to provide insights to create rules that could predict 85% of historically approved fraud transactions.
- Simility's new rules and models were predicting 6X more suspicious transactions in live data. Upon manual review, 68% of these transactions led to confirmed fraud.
- Manual reviews were reduced by 70%. This was primarily attributed to the improved accuracy of the Machine Learning models.

simility

About us: Simility transforms fraud prevention with a versatile platform that combines the best of human analysis and machine learning. To learn more, please visit Simility.com

CONTACT US FOR A DEMO

simility.com/demo