4 Helpful Ways to Use Machine Learning for Fraud Detection

Case IQ

1

Detect Account Takeover

By studying client data, machine learning models can tell when an account has been taken over by a fraudster. The model learns to identify when a customer makes a transaction that is out of the ordinary for them specifically, not based on general rules for every client.

For instance, changes in the following may indicate fraud:

- Location
- Sign-in device for online accounts
- Number of transactions
- Transaction value
- Shipping address

2

Spot Fake Accounts

Fraudsters create synthetic identities using a combination of real and fabricated information to open lines of credit, bank accounts and more.

Creating fake accounts helps fraudsters bypass purchase limits for highly sought-after items, such as luxury handbags and electronics, so they can resell them. Finally, fraudulent accounts on social media and review sites can boost or damage a product or company's reputation through likes and comments.

Machine learning models can spot fake accounts by noting:

- Number of new accounts created at once
- Age of account
- Account activity
- Number of accounts from one IP address

3

Recognize Payment Fraud

Payment fraud includes paying with stolen credentials, return fraud and requesting fraudulent refunds.

Machine learning recognizes payment fraud by spotting suspicious information such as:

- Shipping and billing address that don't match
- Frequent returns or denials of delivery
- Account login on a different device or IP address
- Unusually large or frequent orders
- High number of failed or cancelled transactions
- Orders on one account paid with different credit cards

4

Reduce Promotion Abuse

A fraudster commits promotion abuse when they receive special sales or promotions through fraudulent means. For example, if you offer 30% off a customer's first order, they may create multiple accounts with different credentials to get the discount many times. Or, if a customer gets a reward for every referral they bring in using a personalized discount code, they may create fake accounts or use bots to get the referral bonuses.

Machine learning can spot promotion abuse by recognizing multiple accounts from one network, many accounts that were created in a short time frame, accounts or emails with fraudulent-looking names (e.g. random letters and numbers), and numerous accounts with the same shipping address.