Detecting Credit Card Fraud

Mark Cohen
Springboard School of Data

$30 billion

Estimated worldwide cost of credit and debit card fraud, 2019[1]

[1] https://www.cnbc.com/2021/01/27/credit-card-fraud-is-on-the-rise-due-to-covid-pandemic.html

The Problem

Timing: weeks later vs. at time of transaction

The goal: flag transactions for follow-up

Results: catch ¾ with 11 false positives per hit

Data

Synthetic Data

- Simulated transactions produced by team at IBM
- Why synthetic? Privacy concerns
- 20 million transactions for 2,000 U.S.-based customers

What’s in the data

- Transaction records:
  - Amount, type and location of merchant, mode of transaction, target label (fraud or not)
- Card records:
  - Kind of card, credit limit
- User records:
  - Home location, income, age, sex

Imbalance

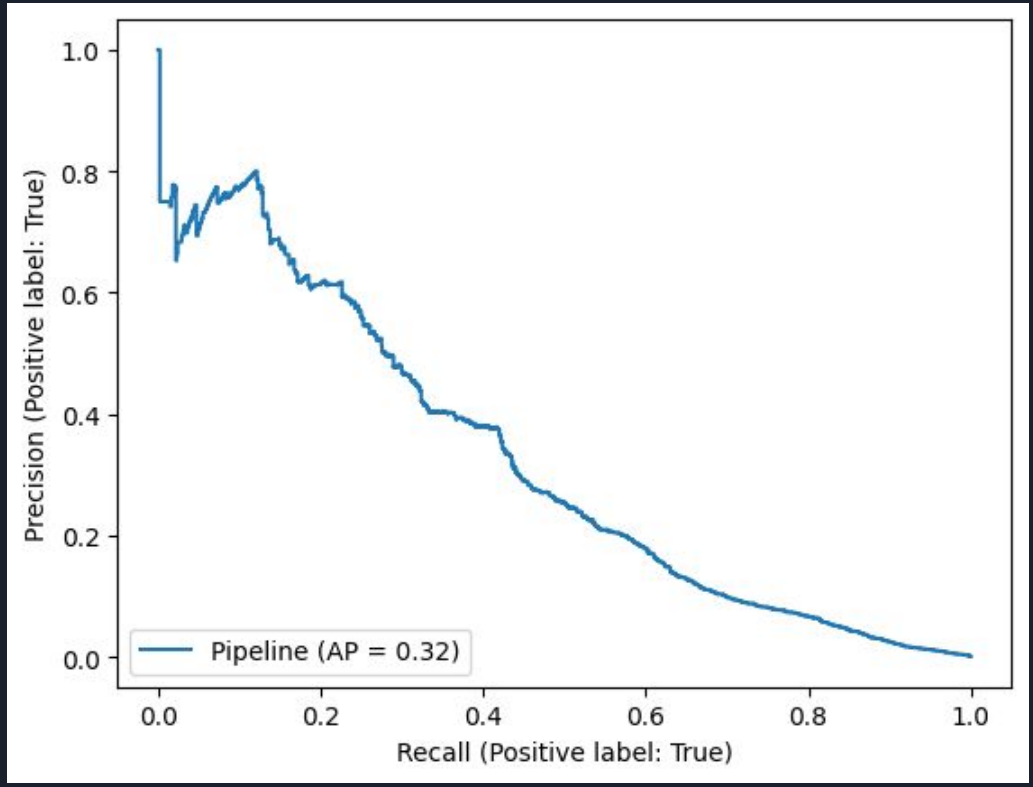
- A problem
  - Around 0.1% of transactions are fraudulent
- Solution
  - Randomly match all 13,850 records of fraudulent transaction in training data with non-fraudulent cases
- Testing data
  - 10% of users

The Model

XGBoost

With 75% recall for positive cases, around 9% precision

11 false positives for each case of fraud caught



Most Informative Features

- Where did the transaction occur?
  - User’s home zip/city/state?
  - In U.S. or overseas?
  - Risk of merchant type (MCC)
- What kind of transaction?
  - Online, chip, or swipe

Recommendations

Warning flags, not definitive labels

Models identifies transactions at higher risk of fraud

Card issuer can follow up to confirm, e.g. with text message

Minor inconvenience outweighed by benefit for customers, issuers, and merchants

Possible extensions

Other modeling techniques, such as recurrent neural networks

“Privacy safe” version of model that could be used by merchants

Summary

- Flagging transactions in real time
- Trading-off catching with inconvenience of false positives