AI and Fraud Detection

Sumedha Rai

AI Researcher

Acorns Grow

New York University (Center for Data Science, Langone Health)

Disclaimer: The views and opinions expressed in this presentation are those of the speaker and do not reflect the official policy, position, or views of any affiliated organization, employer, or institution.

Why is fraud detection important?

- An important topic now more than ever
- Consumers and businesses increasingly expect seamless access to digital integrated financial services
  - Real time online payments, digital deposits, mobile banking, digital wallets
- The same technology that powers this convenience is also exploited to craft increasingly sophisticated fraud schemes

2024

FTC: $12.5 billion over fraud losses

Payment fraud: ~$2.1 billion

Different kinds of fraud?

Account Takeovers

Identity Theft

First Party Fraud

Credit Card Fraud

Wire Transfer Fraud

Traditional approaches may not work?

Manual Reviews

- Struggle to keep up with the volume of digital activity
- Prone to human error, oversight, and fatigue

Rule based Systems

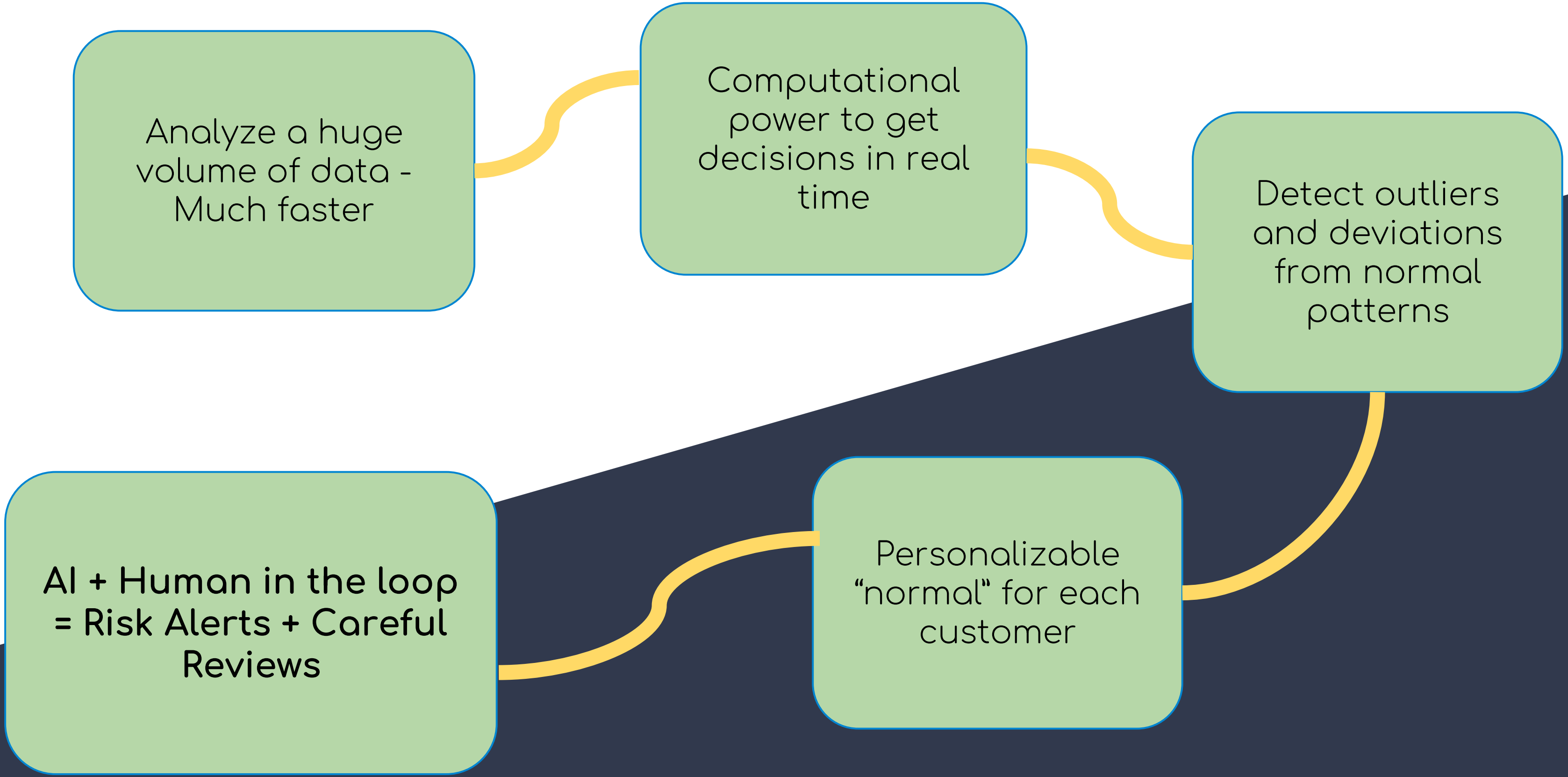
- Hard to maintain as fraud tactics evolve and miss novel fraud patterns, if static
- Generate excessive alerts and false positives, eroding customer trust

Fragmented Data and Lack of Context

- Isolated signals and siloed data points fail to analyze patterns across the entire transactional journey of a user
- Hinders real-time, adaptive fraud detection

Paypal
Stripe

How can AI help?



Analyze a huge volume of data - Much faster

Computational power to get decisions in real time

Detect outliers and deviations from normal patterns

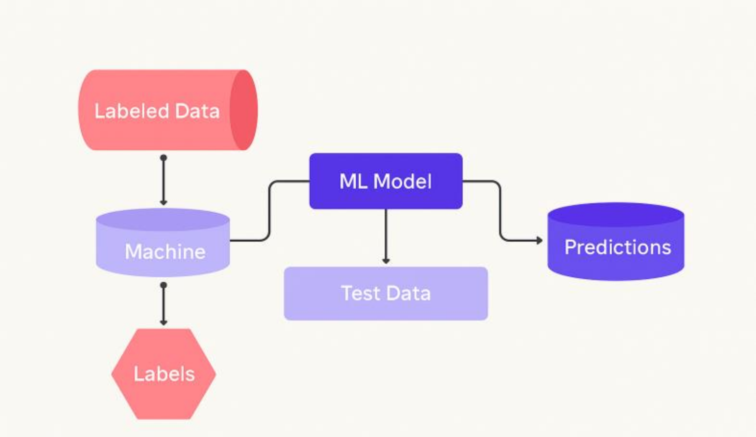
Personalizable “normal” for each customer

AI + Human in the loop = Risk Alerts + Careful Reviews

Techniques/ Algorithms

Supervised Learning Algorithms

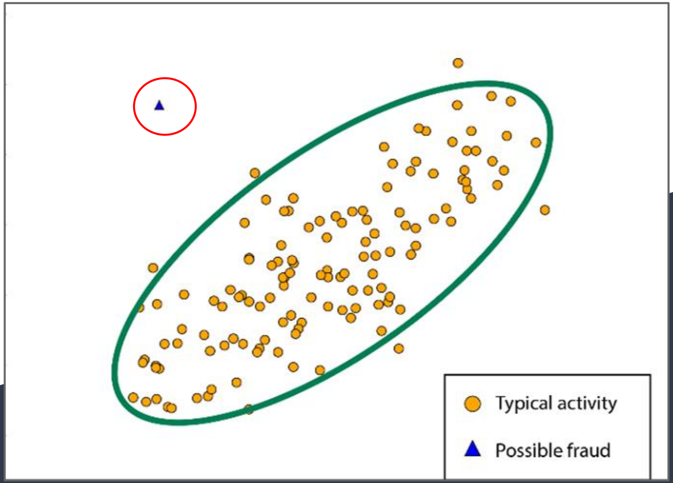
- Trained on labeled historical data - “fraud” or “legitimate”
- Logistic regressions, tree based models, neural networks
- Models can classify new activity/ transactions as high risk or relatively safe



- Great at (real time) transaction monitoring
- Can analyse hundreds of features related to a transaction at the same time

Techniques/ Algorithms

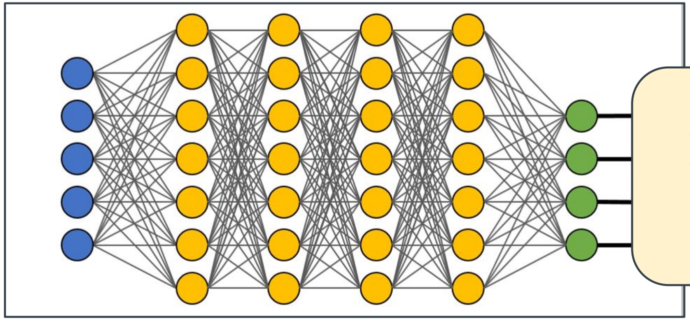
Unsupervised Learning Algorithms



- Can help to find patterns on unlabeled data and pick up outliers or "deviations" from "normal" behavior
- Fraudsters may not have knowledge of past activity - unusual activity can be flagged

- Can work for catching "emerging" or "new" fraud techniques
- Can be early warning signs for possible risky behavior

Techniques/ Algorithms



Deep Learning Approaches

CNNs and vision based models: Identity verification

NLP models: Email phishing/ chat logs/ KYC details

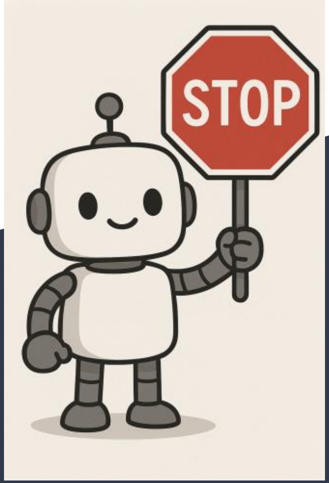
Graph neural networks: Fraud rings/ collusive fraud/ money laundering

Challenges?

How real time can you get?

Interpretability, XAI

Rapidly evolving fraud



Data Quality

Feedback?

Class imbalance

High false positive rates

Adoption

Build

vs

Buy?

Complexity of Solution

Data needed Consortium? proprietary?

Cost benefit analysis

Control over solution

Ethical use of AI

Data Security

Data Privacy / PII

Bias and discrimination

Transparency

Human in the loop!

Thank you!

Questions?