Fast Fraud Screening

Using Lightweight Models to Flag Risk Before Deep Analysis

Abdullah Ahmed
Noimot Bakare Ayoub
Cyril Cordor
Brandon Owens

THE ERDŐS INSTITUTE
Helping PhDs get and create jobs they love at every stage of their career.

Motivation

Money moves everything, which makes protecting it everyone's business.

- Financial fraud continues to cost institutions billions globally every year.

- As digital transactions surge, fraudsters are becoming more sophisticated.
- Traditional systems struggle to keep up with adaptive fraud tactics.

- Fast, accurate, and efficient systems that can identify suspicious behaviour early are needed.

How can we make existing, computationally intensive fraud detection pipelines more efficient with minimal changes to their current architecture?

Solution:

Build a lightweight, flexible, preprocessing model that filters out low-risk cases before the pipeline.

Data Overview

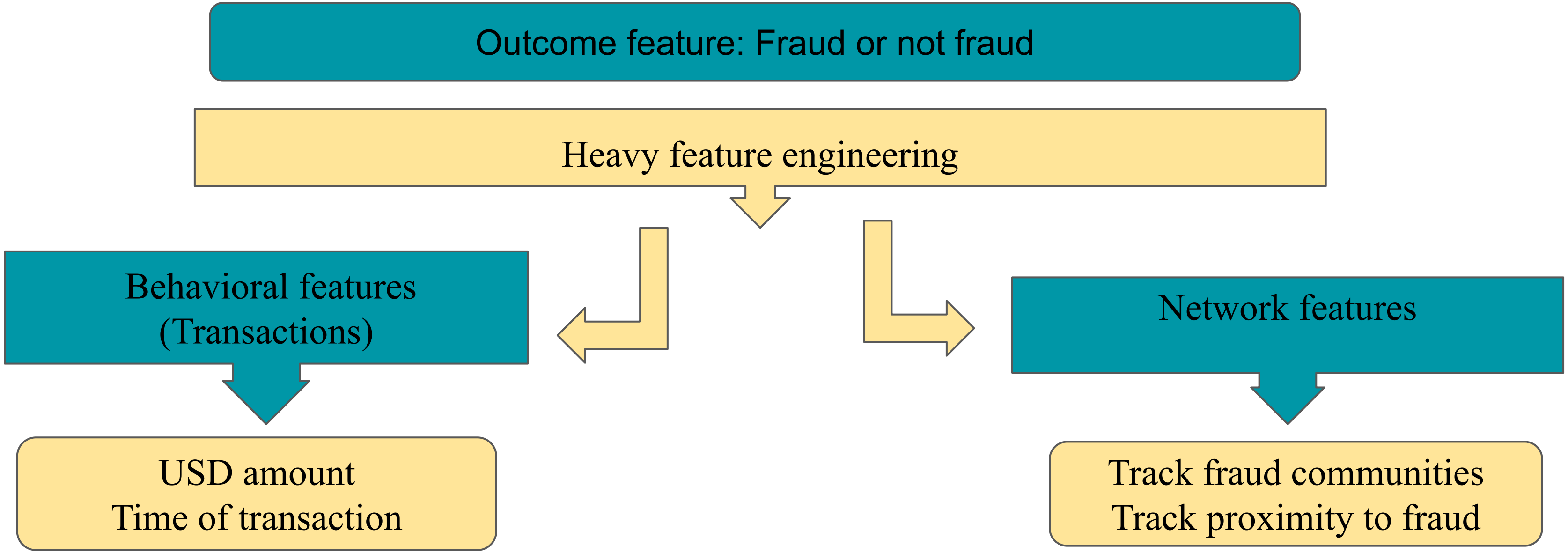
- Synthetic data by [JPMorganChase Payment Data for Fraud Protection]
- Mimics real world transaction patterns, and fraud behavior
- The dataset contains ~ 1.49 million transactions
- Covers a period of approximately 50 years.

Transaction_Id	Sender_Id	Sender_Account	Sender_Country	Sender_Sector	Sender_lob	Bene_Id	Bene_Account	Bene_Country	USD_Amount	label	Transaction_Type
PAY-BILL-3589	CLIENT-3566	ACCOUNT-3578	USA	21264	CCB	COMPANY-3574	ACCOUNT-3587	GERMANY	492.67	0	MAKE-PAYMENT
WITHDRAWAL-3591	CLIENT-3566	ACCOUNT-3579	USA	18885	CCB				388.92	0	WITHDRAWAL
MOVE-FUNDS-3528	CLIENT-3508	ACCOUNT-3520	USA	4809	CCB	COMPANY-3516	ACCOUNT-3527	GERMANY	280.7	0	MOVE-FUNDS
WITHDRAWAL-3529	CLIENT-3508	ACCOUNT-3519	USA	7455	CCB				118.14	0	WITHDRAWAL
QUICK-DEPOSIT-3471						CLIENT-3442	ACCOUNT-3461	USA	105.16	0	DEPOSIT-CASH
QUICK-DEPOSIT-3473						CLIENT-3442	ACCOUNT-3460	USA	164.97	0	DEPOSIT-CASH
PAY-BILL-3404	CLIENT-3384	ACCOUNT-3395	USA	36316	CCB	COMPANY-3392	ACCOUNT-3401	GERMANY	456.89	0	MAKE-PAYMENT
QUICK-DEPOSIT-3406						CLIENT-3384	ACCOUNT-3396	USA	413.17	0	DEPOSIT-CASH
PAY-CHECK-3347	CLIENT-3330	ACCOUNT-3341	USA	36194	CCB	CLIENT-3333	ACCOUNT-3338	CANADA	377.65	0	PAY-CHECK
PAY-CHECK-3348	CLIENT-3330	ACCOUNT-3340	USA	20626	CCB	CLIENT-3333	ACCOUNT-3338	CANADA	338.03	0	PAY-CHECK
MOVE-FUNDS-3292	CLIENT-3272	ACCOUNT-3284	USA	21568	CCB	CLIENT-3275	ACCOUNT-3291	CANADA	100.85	0	MOVE-FUNDS
MOVE-FUNDS-3294	CLIENT-3272	ACCOUNT-3284	USA	29040	CCB	CLIENT-3273	ACCOUNT-3289	USA	276.66	0	MOVE-FUNDS
PAY-BILL-3232	CLIENT-3203	ACCOUNT-3222	USA	27393	CCB	COMPANY-3210	ACCOUNT-3218	GERMANY	234.88	0	MAKE-PAYMENT
QUICK-DEPOSIT-3234						CLIENT-3203	ACCOUNT-3222	USA	945.22	0	DEPOSIT-CASH
DEPOSIT-CASH-3163						CLIENT-3139	ACCOUNT-3154	USA	655.09	0	DEPOSIT-CASH
PAY-BILL-3162	CLIENT-3139	ACCOUNT-3153	USA	25066	CCB	COMPANY-3147	ACCOUNT-3160	GERMANY	675.37	0	MAKE-PAYMENT
WITHDRAWAL-3100	CLIENT-3075	ACCOUNT-3090	USA	22778	CCB				319.95	0	EXCHANGE
QUICK-PAYMENT-3099	CLIENT-3075	ACCOUNT-3091	USA	39013	CCB	CLIENT-3078	ACCOUNT-3087	TAIWAN	771.54	0	QUICK-PAYMENT
PAY-BILL-3036	CLIENT-3016	ACCOUNT-3028	USA	43951	CCB	COMPANY-3022	ACCOUNT-3033	GERMANY	730.69	0	MAKE-PAYMENT

Note: Timestamp feature provided and data is sorted by timestamp

Image source: JPM Chase

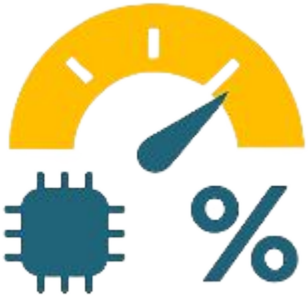
Modeling Approach



Concurrent feature generation with network updates to prevent data leakage.

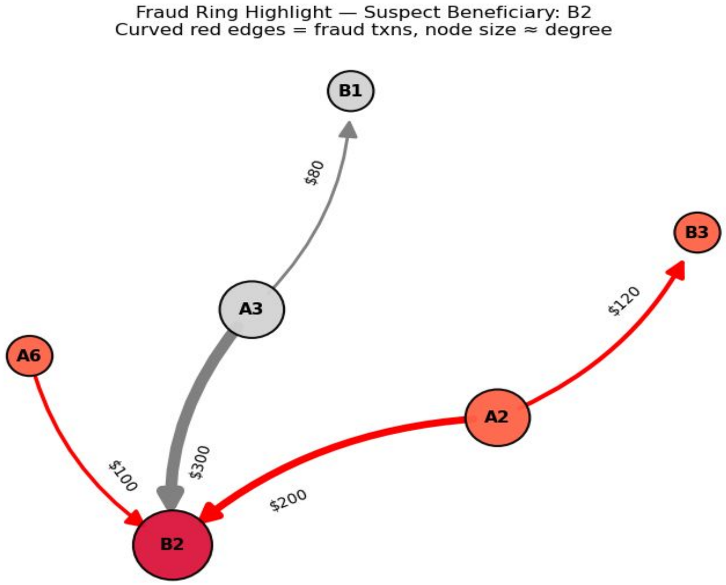
Each transaction is processed sequentially: feature generation, prediction, and network update.

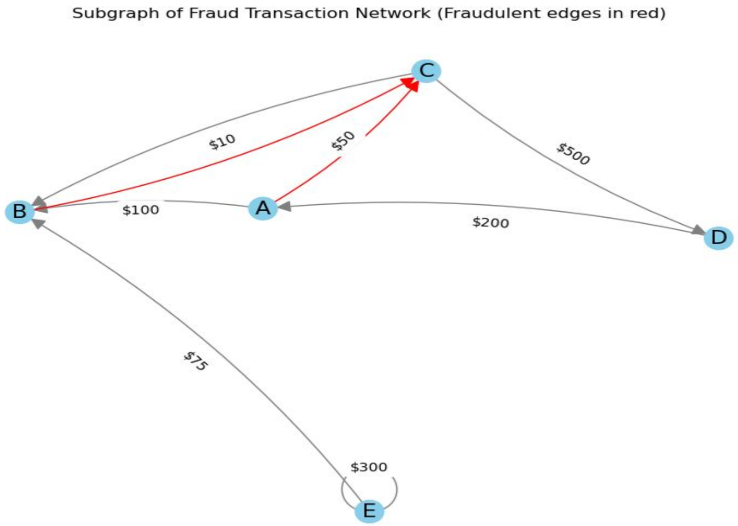
Modeling Framework



Using NetworkX

- We analyze how accounts and users connect.
- Fraud often happens in clusters
  - Suspicious accounts interact frequently
  - Cycle funds among themselves
- Network view exposes hidden connections and abnormal patterns.





In this network:

- Nodes represent entities (sender and beneficiary accounts)
- Edges represent transactions between them.
- Multiple edges indicate repeated activity (ex. multiple transfers between the same pair)
- Direction shows who sent versus who received

Data Disclaimer: The values used to construct these network images are synthetic and were generated to simulate fraud ring patterns for demonstration purposes only.

Evaluating Performance

Why Traditional Metrics

Challenges with Accuracy, Recall and PR-AUC

- **Problem:** Class imbalance (~2% fraud) → High accuracy is misleading
- **Why Metrics Fails:** Accuracy, Recall, PR-AUC don’t reflect real world fraud detection needs.
- **Proposed Metric: Lift = Recall/Predicted Positive Rate ~ Efficiency of filter.**

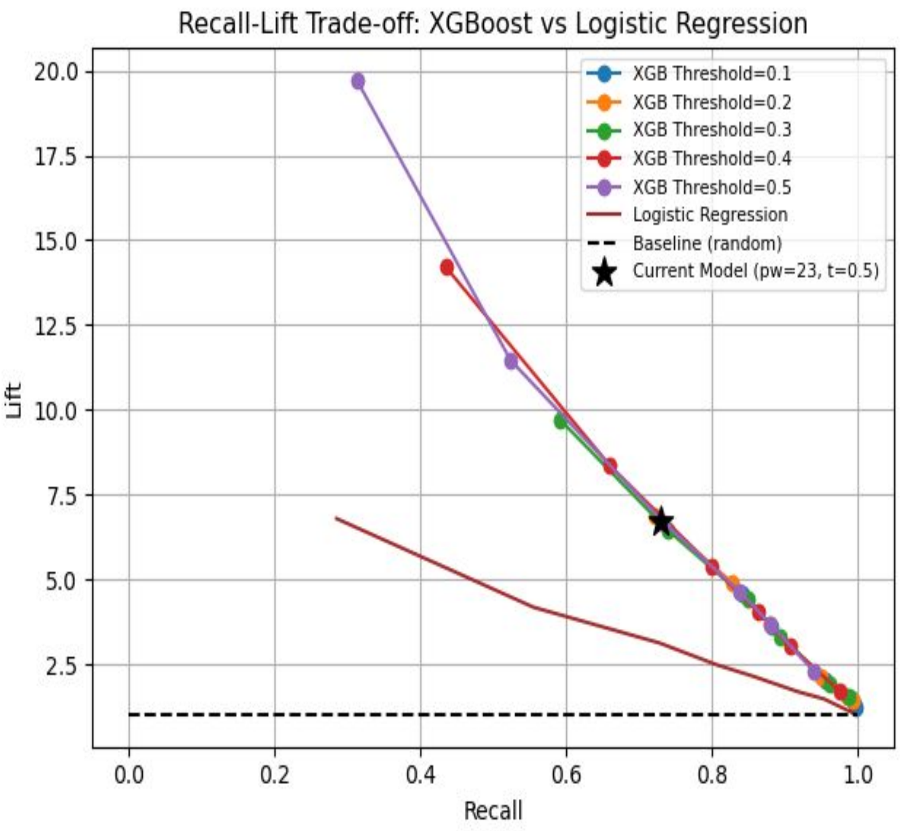
$$\boxed{\text{Lift} = \frac{\text{Recall}}{\text{Predicted Positive Rate}}}$$

Model performance and calibration

- Businesses priority is maximizing fraud detection while maintaining actionable lift.

- **XGBoost (example):**
  - **Lift: 7x**
  - **Recall: 73%** - catches a majority of fraud cases
  - Catches 3 out of 4 fraud cases with 7x better targeting than random

- We can evaluate lift-recall trade-offs across models for optimal business performance.



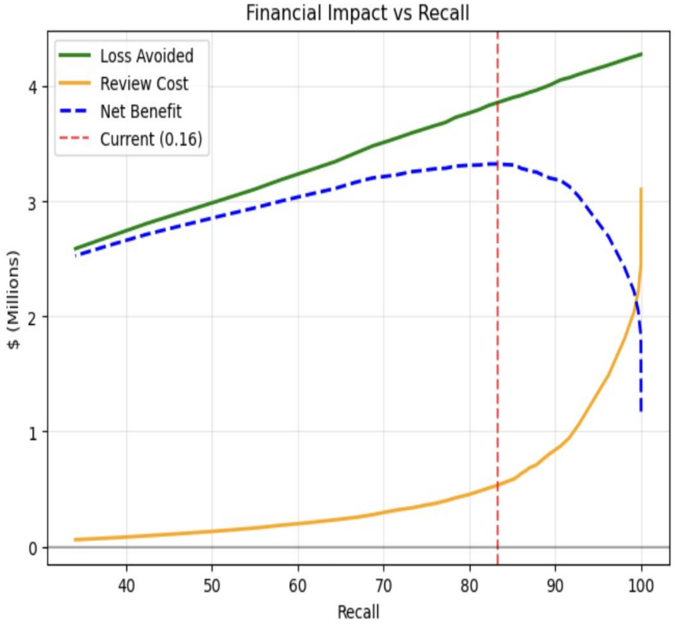
Note: Variable recall is achieved by adjusting the positive class weight (scale_pos_weight (pw))) across models. Each curve corresponds to a fixed classification threshold. Threshold choice doesn't dramatically change the recall-lift curve, they overlap.

Business Deployment (KPIs)

Business goal → high efficiency

Metric	Result	Interpretation
Fraud Detection Recall	83%	% of fraud successfully flagged
False Negative Rate	17%	% of fraud missed
False Positive Rate	16%	% of legitimate transactions flagged
Synthetic Loss Avoided	$3.8M	Proxy dollars saved by catching fraud
Total Review Cost	$0.53M	Cost of analyst reviewing alerts
Missed Fraud Risk	$0.47M	Proxy dollars lost from missed fraud

Threshold	Recall	Lift	% Flagged	Loss Avoided	Net Benefit
0.00	100.0%	1.00x	100.0%	$4.27M	$1.17M
0.16	90.6%	3.22x	28.2%	$4.05M	$3.18M
0.18	89.3%	3.44x	25.9%	$4.01M	$3.20M
0.20	88.4%	3.68x	24.0%	$3.98M	$3.23M
0.30	85.7%	4.32x	19.8%	$3.91M	$3.30M
0.36	83.3%	4.84x	17.2%	$3.86M	$3.32M
0.40	81.2%	5.23x	15.5%	$3.80M	$3.31M
0.50	74.5%	6.51x	11.4%	$3.62M	$3.26M
0.60	66.8%	8.14x	8.2%	$3.42M	$3.17M
0.70	50.4%	11.64x	4.3%	$2.99M	$2.86M



*Note: Institutions select optimal parameters; we use optimization .36. **Assumptions:** Synthetic business metrics are based on a synthetic JPMorgan Chase analyst earning $50/hour, taking 15 minutes per case review, and an initial triage cost of $12.50.*

Limitations, Conclusion & Future Work

Limitations

Results based on simulated data may not capture real world fraud complexity and revolving tactics.

16% false positive rate still creates operational burden and potential customer friction from legitimate transaction reviews

Class imbalance (2% fraud) makes achieving both high recall and high precision mathematically challenging

Conclusion

Serves as an effective first-layer filter in fraud detection

Enhances fraud detection by prioritizing high risk cases

The benefits of our model goes beyond the 3.3M saved:

- Customer trust
- Brand reputation
- Regulatory Compliance

Future Work

Integrate real world data for better robustness

Incorporate weekly retraining for continuous adaptation

Explore advance models to reduce false negatives

Acknowledgments

Steven Gubkin & Alec Clott

Erdös Institute - Guidance & Support

Olivier Binette

Project Mentor - Insightful Direction

JPMorgan Chase

Data Powering Our Analysis