Team 20 Introduces FraudBot to Enable Financial Institutions to Detect Fraudulent Activity

FraudBot provides faster detection of fraudulent transactions.

Knoxville, TN - 12/3/24 – FraudBot, introduced by Team 20, is a fraud detection machine learning model that allows financial institutions to easily classify any given transaction as fraudulent. FraudBot identifies accounts with a higher likelihood of fraud, allowing our clients to better protect their clients. FraudBot gives institutions the ability to focus and cater the model to their consumer base.

Customer Problems:

- 1. Credit card fraud has affected one quarter of all card holders in the previous year making it the most common form of bank fraud.
- 2. The sheer amount of raw transactional data makes human verification of real transactions impossible.
- 3. Subtle signs of fraudulent transactions are easily missed by manual reviewers, but with machine learning we can uncover these patterns.

FraudBot provides an interface for storing and analyzing transactional data. This tool harnesses the functionality of deep learning to accurately predict fraudulent transactions in a consumer's history. FraudBot benefits from the sheer amount of raw transactional data by learning the subtle signs of fraudulent transactions better than any manual reviewer. This product is similar to Amazon's Amazon Fraud Detector that also uses the power of machine learning to classify fraudulent transactions.

"As the CEO of FraudBot, I believe that true leadership is about empowering others to take control of the challenges they face. Our mission isn't just to stop fraud—it's to equip financial institutions with the tools and confidence to protect their customers in a rapidly changing world."

— Ryan Franqui, CEO, FraudBot

Consumers:

FraudBot makes the job of the financial institution much easier. Consumers can use FraudBot out of the box, instantly improving their security and protection. Those with larger or

specialized consumer bases can take advantage of FraudBot's downstream training capabilities, focusing the model to their needs.

"As a regional bank, our biggest challenge was staying ahead of increasingly sophisticated fraud attempts while maintaining a seamless experience for our clients. We needed a solution that could not only detect fraud but also adapt to the unique behaviors of our customers. FraudBot has done exactly that. It's helped us cut down on false positives and identify real threats faster, all while giving us the flexibility to fine-tune the model for our specific needs. Fraud prevention has never been easier or more efficient for our team."

— Jessica M., VP of Risk Management at Horizon Bank

FAQs

1. Who is your customer? Who will be using your product?

Our customers are financial institutions. Specifically, financial institutions or banks who handle large amounts of transactional data which could be fraudulent.

2. How does your product make your customer's life significantly better? What is the problem to solve?

FraudBot will help identify the most popular form of identity theft, a potentially life ruining problem affecting nearly a quarter of our customers' clients.

3. Why is this a problem that needs to be solved right now?

The faster fraud can be detected the more damage can be minimized. By improving the way that fraud is recognized we can potentially protect millions of clients personal and business financial assets.

4. What might disappoint the customer?

By the nature of training a machine learning model, the customers' clients lose anonymity in their transactional data, letting Fraudbot learn off of their spending habits.

5. How will the customer discover or find our product? Is this a web, mobile, desktop, or a specialized tool/app?

Our application will work best as a specialized tool for only the bank to use because of the sensitive nature of the work Fraud Bot does. This can be advertised at financial conventions.

6. How will you measure success?

Success can be measured by reducing false positives and increasing true positives in credit card fraud detection. This metric allows us to compare to other fraud detection services.

7. What are the baseline model(s) and paper(s) you will use for inspiration?

We are inspired by models like Amazon's Fraud Detector and various machine learning models utilized for fraud detection in the finance industry.

8. What is the dataset for your project?

We are using the Credit Card Fraud dataset from Kaggle.

9. What are the computational needs for your idea?

The project will require GPU-accelerated computing for training deep learning models on large datasets, along with scalable cloud storage to handle high volumes of transactional data.

10. What are the key milestones in your roadmap:

	Milestone/Feature Description	Priority	Deadline
1	Filter and Clean Dataset	Med	9/25/24
2	Literature Review	High	10/1/24
3	Experiment with Various Models	High	10/10/24
4	Experiment with Various Loss Functions	Low	10/10/24
5	Baseline Model (Model Training on initial dataset)	High	10/20/24
6	Midterm Project Report	High	10/20/24
7	Review and Expand Baseline Model	Med	10/31/24
8	Generate a new dataset to test the model on	Med	11/5/24
9	Test accuracy of model on the generated dataset	Low	11/5/24
10	Retrain the model on the generated dataset	Med	11/10/24
11	Test the accuracy of the final model	High	11/26/24
12	Delivery of project presentation	High	11/26/24
13	Delivery of final project report	High	11/29/24