EasyChair Preprint

№ 11689

Open AI and Its Impact on Fraud Detection in Financial Industry

Sina Ahmadi

January 4, 2024

ISSN: 2959-6386 (Online), Vol. 2, Issue 3, December 2023

Journal of Knowledge Learning and Science Technology

journal homepage: https://jklst.org/index.php/home

Open AI and its Impact on Fraud Detection in Financial Industry

Sina Ahmadi

Independent Researcher

Abstract

As per the Nilson report, fraudulent activities targeting cards amounted to a loss of $32.34 billion globally in 2021, a 14 % increase from the previous year. Such practices can be combated by harnessing OpenAI's powerful machine learning and automation capabilities. Such advanced technologies help financial companies avoid any potential fraud and protect their esteemed clients' interests. Through the adoption and utilization of such innovative technologies., financial institutions will be better placed to protect their customers and entities from financial losses. Digital fraudsters are skilful in identifying loopholes and have developed cunning techniques like phishing for unsuspecting victims and wittingly swindling money off them. They are also updated in using OpenAI to develop deceitful information to scam people. This has seen the emergence of names like WormGPT and FraudGPT, reliant on generative AI models used by tech corporations with fraud intents. As a result, fraud detection techniques have to evolve with time as fraudsters progressively devise new techniques that bypass old and rigid banking security protocols and learn how to convince unsuspecting individuals to dispatch their money to them.

Keywords: OpenAI; machine learning; fraud; fintech

Article Information:
Article history: *Received:* 15/06/2023 *Accepted:* 30/08/2023 *Online:* 20/09/2023 *Published*: 12/12/2023
DOI: https://doi.org/10.60087/jklst.vol2.n3.p281
[i] **Correspondence author:** Sina Ahmadi Email: sina0@acm.org

Introduction

Due to its vast implications, fraud is one of man's biggest problems. It refers to intentionally using false details to swindle an organization, individual property or money. The COVID-19 pandemic saw an upsurge in fraudulent malpractices due to the economic recession that most unemployed individuals faced (G. Colvin 2020). The pandemic had rendered thousands of individuals jobless, while those privileged to be working faced cuts in their salaries. Fraud experts say fraud springs from three elements: opportunity, pressure and rationalism (A. Littman 2011). Fraud also occurs when a person develops an unshakeable urge or motive to commit fraud.

The likely fraud perpetrator needs to feed an unmet urge with limited resources. These unmet needs continue to grow as they are endless and different among people. They may include gambling debts, reduced household income or burgeoning medical bills. Once the person encounters such unmet needs and has

limited resources to meet them, they may opt for fraud. Opportunities are expressed as a lack of internal controls or reckless management within a person that may present fraud as an easy activity. Lastly, the person rationalizes their intent to engage in fraudulent activities by assuring themselves that they urgently needed the money or would eventually pay it back. With harsh economic spells, there is increased motives and pressure to engage in fraud, pushing the fraudsters to rationalize their actions.

Fraud is common in finance and comprises money laundering, financial statements fraud, email phishing, cyber fraud, and credit card fraud. The advent of digital banking exposed financial institutions to digital fraud. It therefore becomes necessary to acknowledge that fraud management is essential in the finance docket, though it is an excruciating venture. Digital fraudsters are skilful in identifying loopholes and have developed cunning techniques like phishing for unsuspecting victims and wittingly swindling money off them. As a result, fraud detection techniques have to evolve with time as fraudsters progressively devise new techniques that bypass old and rigid banking security protocols and learn how to convince unsuspecting individuals to dispatch their money to them.

Traditional fraud detection approaches within the finance docket are rule-based, meaning that humans make the rules. Most financial institutions use such approaches. As more people opt for emerging digital technologies, fraud scenarios are projected to increase, rendering the existing rule-based approaches unsustainable and unscalable. Additionally, false positives (non-fraudulent practices termed as fraudulent) impose substantial financial losses in terms of customer complaints and transactions in the finance sector. Ciabanu's 2020 study on 1000 adult customers discovered that almost 25 % of the customers whose transactions had been falsely declined turned to competitors for the same financial services (M. Ciobanu 2020). The switch of competitors increased to 36 % for the customers between 18 and 24 years and a further 31 % for those in the 25-34 years old bracket (M. Ciobanu 2020). Such results show the profitability needed for modern fraud detection structures.

Financial, banking and fintech industries encounter various scams annually. The scams can be categorized into these classes: digital fraud, physical attacks, internal collusion and violation of the Four Eyes Rule. The last two items involve employee-based schemes or traditional malpractices. Digital fraud, however, involves a range of online fraud activities. Machine learning and automation are needed to combat digital fraud as they have evolved into crucial business tools as fraudsters develop increasingly intricate practices. Such advanced technologies help financial companies avoid any potential fraud and protect their esteemed clients' interests. Through the adoption and utilization of such innovative technologies., financial institutions will be better placed to protect their customers and entities from financial losses.

To add to the challenges encountered by the traditional rule-based system, fraudsters need specific patterns and keep changing their hacking techniques. This renders the system cumbersome and quickly

obsolete. There arises the need to change this traditional approach in any financial institution. As per the Nilson report, fraudulent activities targeting cards amounted to losses of $32.34 billion globally in 2021, a 14 % increase from the previous year (C. Mullen 2023). With the increase in technological processes in the banking sector and due to the diverse payment channels, such as debit and credit cards and smartphones, the number of digital transactions has increased since 2020. Due to such occurrences, there is a dire need to create more robust and rigid fraud detection solutions in the financing world. The onset of AI has opened a myriad of approaches to adopting and curbing these online malpractices.

Technological giants like Google, Facebook, Apple, Amazon and Netflix have also leveraged proprietary AI tools to improve their back-end and front-end financial processes. Currently, they have prioritized using AI in their financial strategies by frequently collecting and using new data to serve through AI models, which has set the bar for the economic world in fraud detection.

Fraud Detection in the Finance Industry

An article in Javelin Strategy and Research on fraud detection claims that fraud detection in financial institutions uses a brick-and-mortar model, which takes much longer to implement (Pascual et al. 2017). Such long durations could be more welcoming for the financial institutions and their customers since several dire fraudulent malpractices could be affected within these durations. Fraud also hugely affects financial institutions that are involved in online payment services, mainly under the contemporary technological advancement in the business industry. For instance, almost 20 % of customers change financial institutions after encountering fraud (S. Sando 2021). The defection of such members to rival institutions causes financial losses and bad reputations to the victim institution, mainly if the trend becomes recurrent. It, therefore, becomes an essential practice for financial institutions to mount robust fraud detection structures within their systems. There are two major fraud detection approaches, the rule-based approach and the leveraging of OpenAI.

Machine Learning-Based Fraud Detection

There are hidden and disguising events in user behaviour that lack the clarity of outright evidence to be identified as fraudulent transactions. Machine learning allows for the development of algorithms that can handle massive datasets with several variables and helps identify these hidden behaviours between operator behaviour and the likelihood of fraudulent actions. Machine learning structures are more advanced than traditional rule-based structures due to their fast data processing capabilities and automation tools in data handling. For example, intelligent algorithms are excellent in behaviour analytics as they reduce the number of verification steps needed.

Financial institutions are more involved in monitoring the likely occurrence of fraudulent activities as they must identify and communicate any flagged online activity. A research by Villalobos explains a scenario that involved the programming of a machine prototype on a dataset containing transactions that had been criminally executed. The prototype used in the rule-based model helped identify the hidden relations manifested in the transactions and criminal activities. Such machine learning systems reduce the amount of work in smaller financial institutions that undertake fraud monitoring operations. The suggested solution in the article revealed that 99.6 % of money laundering transactions and cut down the reported transactions from 30 % to 1 % (Villalobos and Silva 2017).

Machine learning (ML) is built on algorithms, which increase efficiency as the data size increases. The greater the data, the more the machine learning prototype grows more efficient and can differentiate the differences and similarities between different behaviours. The more the machine learning model unearths the differences between fraudulent and legitimate operations, the more its systems grow more efficient in sorting data sets into the needed classes. Machine learning models become more scalable as the customer database increases in size.

Although machine learning algorithms have numerous benefits in fraud detection among financial institutions, they carry some drawbacks that limit their application in detecting fraud. For example, one of the main disadvantages is that machine learning needs colossal amounts of data for the models to be accurate. The data threshold is manageable, but there should be ample data points that identify the legitimate causal associations in smaller financial institutions. In addition, machine learning algorithms run on actions, activity and behaviour. The model may overlook clear connections, for instance, a card used in multiple accounts, which could render the fraud detection operation inaccurate.

Article Reviews

Ayowemi (Awoyemi, et al. 2017) researched why credit card-related fraud detection becomes an impediment and articulated that it occurs for two main reasons. Firstly, fraudulent and regular behaviour changes constantly. Secondly, there is a massive imbalance in the datasets generated from credit card fraud. In the same vein, the approach used to sample the dataset, the selection of variables and the methods used in fraud detection also affect the fraud detection performance in transactions related to credit cards. The research investigated the performance of naïve Bayes, k-nearest Neighbour and logistic Regression on credit card datasets assumed to be largely skewed. The research also uses a hybrid technique that involves the undersampling and oversampling of skewed data. The techniques were applied to the generated data and later transferred to Python. The results demonstrated higher levels of accuracy for k-nearest Neighbour, naïve Bayes and classifiers for the Logistic Regression were 97.92 % and 97.69%. According to the

comparative results, k-nearest Neighbour outperformed the naïve Bayes and Logistic Regression algorithms.

Research carried out by Bauder et al. focused on the alleged fraud experienced at Medicare. The research compared some of the machine learning methods leveraged while identifying fraud at Medicare. The researchers carried out a comparative study using hybrid machine learning methods that relied on four performance systems of measurements and minimization of class imbalance by deploying the 80-20 undersampling technique in tandem with oversampling. The former sampling technique had a better performance than the latter approach. The research concluded that oversampling leads to poor performance in machine learners (Herland 2018).

To add to this pool of research, balanced accuracy (BACC) seemed unreliable as a method of measuring the performance of models in various models and rendered it unable to reflect more realistic alterations observed in other metrics. Therefore, the undersampling technique enhanced learner performance and the supervised approaches turned out better than the hybrid and unsupervised hybrid learners. The provider section contributed to impediments in fraud detection, with somewhat specialized provider categories depicting higher performances than other general categories.

Use of Generative AI in augmenting and enhancing fraud detection strategies

Generative AI's backbone involves the use of transformer deep neural networks. One such example of generative AI is OpenAI's ChatGPT. Generative AI is constructed to provide data sequence as output and has to be trained using sequential data, like payment histories and sentences. It varies from other methods that produce single categorizations, such as fraud/ not fraud, depending on the given input and training data, that can be provided to the model in any sequence. Generative AI's yield can progress indefinitely, while other classification methods only yield single outputs.

Generative AI becomes the superlative tool needed to generate data grounded on actual data synthetically. Its development will depict essential applications in detecting fraud, whereby, as earlier noted, the number of feasible fraud samples remains little and challenging for machine learning to effectively learn from., A model can apply generative AI and use the existing patterns to develop novel, synthetic samples that pose as actual fraud samples, enhancing the fraud signals for essential fraud detection machine learning tools.

An archetypal fraud signal comprises non-fraudulent and fraudulent data. Usually, the non-fraudulent data appears first in the sequence of events and carries the actual behavioural activity of the card's owner. Generative AI can generate such payment sequences and simulate a fraud attack on the card, which would then be used to train data to help fraud detection machine learning tools and enhance their performance.

Using Generative AI to detect Fraud

One of OpenAI's criticisms is that current models can rely on incorrect outputs. This is a significant flaw that most people in financial institutions are concerned about as they never use public tools like customer chatbots to present made-up, more false information. However, the perceived flaw can be used to generate synthetic fraudulent data since synthetic disparity in synthesized output can develop exceptional fraud patterns, enhancing the end fraud defence model's detection performance.

As known to many, repetitive examples of a similar fraud signal do not always enhance detection since most of the machine learning models need a few occurrences of each entity to learn from. The variation in the developed outputs generated from the generative model increases the sturdiness of the end fraud model, helping it spot any fraud patterns in the data and identify similar attacks that would have quickly passed unnoticed if traditional processes were used.

This would pose some concerns for fraud managers and cardholders as they may wonder how a fraud model trained on generated data can enhance fraud detection and any merits attached to the exercise. Unknown to them is that before a model is used on live payments, it passes through severe evaluation operations to maintain its projected performance. It is abandoned if it does not attain the expected top-notch performance and replacements are trained until the best models are found. This process is standard and is the norm for all produced machine learning models since models trained using authentic data can also produce substandard results during the evaluation stage.

Tools used in OpenAI to effectively detect Fraud in Finance

Financial institutions are overwhelmingly shifting to AI to help in efficient fraud detection. Multiple industries including banking, fintech and e-commerce have already adopted fraud detection solutions. Using machine learning algorithms, such industries can now process huge amounts of data and detect suspicious patterns to safeguard the business from fraud**.**

The Use of Logistic Regression in Fraud Detection Machine Learning Algorithms

Logistic regression is the supervised learning method supported by definite decisions. All obtained results are categorized as non-fraud or fraud once a transaction occurs. This technique uses a cause-and-effect relationship to generate organized data sets. The regression analysis method is more complex when detecting fraud due to the data set sizes and numerous variables. This algorithm forecasts whether new transactions will be categorized as fraudulent. The models are primarily accurate for clients from larger financial institutions. However, the general models also remain viable and applicable for use.

Using Decision Trees in Fraud Detection Machine Learning Algorithms

This AI version creates a graphic illustration of a decision-making process. They are useful tools in fraud detection, as they did in identifying the most crucial variables that led to fraud and developing a framework used in identifying fraudulent transactions.

Decision Tree algorithms come into play while classifying atypical activities in any transaction an authorized user initiates. The algorithms house trained constraints that are essential tools in fraud classification on the dataset. The algorithms are used in the regression or classification extrapolative modelling challenges. They are fundamental rule sets designed to use fraud allegations involving clients.

Designing a decision tree discards any unrelated features and does not need wide-ranging data normalization. After a tree is inspected, it becomes clear why some decisions were made by relying on the group of rules initiated by a specific client. The machine learning algorithm output may surface as a model aping the decision tree, giving a possible trace of fraud based on earlier events.

Using Random Forest in Fraud Detection Machine Learning Algorithms

Random Forest Machine Learning combines decision trees to produce more accurate results. Every tree assesses transactions for various decisions (V. Ayyadevara 2018). Training is conducted on random datasets. Depending on the executed training offered on the decision trees, each tree classifies transactions by deeming them either fraudulent or non-fraudulent. The model is then harnessed to accurately predict the result, allowing fraud detectors to even out errors that may surface in a tree. It improves the overall performance model accuracy and sustains the ability to interpret the results and give explicable scores to the users.

Random forest runtimes are fast and can handle unbalanced or missing data. However, they have some weaknesses. For instance, when deployed in regression, they cannot predict past the variety in the training of the data and may provide overfit data sets, often termed as noisy.

Using Neural Networks in Fraud Detection Machine Learning Algorithms

They emulate the complex nature of the human brain. Financial institutions use it to parse antique databases of preceding transactions, inclusive of those predetermined as fraudulent transactions. Each transaction a neural network processes upsurges its accuracy levels in detecting future frauds and incorporates it into its vast repository of historical information, enabling the model to learn new and existing patterns of habitual fraudsters continually.

Neural networks are designed to function similarly to the human brain. They utilize various computation layers. They also use cognitive computing that aids in developing machines that can use self-learning algorithms that involve data mining, processing of natural language and recognition of patterns

(D. Graupe 2016). Neural networks pass through multiple layers during the data training process. They however, give more accurate results than other models since they use cognitive computing and learn from the patterns of authorized behaviour. They are therefore able to distinguish between non-fraud and fraudulent transactions. They blend into the change in the behaviour of what is assumed to be standard transactions and identify types of fraudulent transactions. Neural networks are fast and function in real-time.

Deep Learning

Mastercard is one of the leading users of AI in preventing card-related fraud. The adoption of AI technology has helped Mastercard reduce occurrences of false declines. Through the leveraging of deep learning models that progressively learn from the organization's 75 billion transactions processed annually across its 45 million locations worldwide, the AI system uses a constantly flowing stream of data and self-searching algorithms to make its decisions (OpenAI 2023). The results are hugely impressive, significantly reducing fraudulent practices and false declines for Mastercard.

Natural Language Processing

World leading institutions, such as PayPal, American Express and Bank of New York Mellon, are some of the financial institutions using the power of Natural Language Processing in fraud detection efforts (OpenAI 2023). NLP extracts signals from IVR interactions, voice and chats to enable these financial companies to effectively spot and prevent suspicious fraud due to the technology's capacity to enhance routine detection.

Merits of Using AI-Powered Fraud Detection Systems

AI-powered fraud detection approaches create a more efficient strategy than the existing traditional methods as they offer intricate fraud pattern detection and real-time analysis and are adaptable to emerging fraud schemes; by reducing the associated time, budgets and false positives, OpenAI will increase the efficiency and accuracy of detecting fraud, causing to decreased financial losses emerging from cybercrimes.

From a client's viewpoint, institutions that accurately and efficiently detect fraudulent activities will prevent customers from falling victim to financial fraud. Therefore, institutions that adopt OpenAI will benefit from preventing fraud and increasing customer retention and loyalty.

Partnerships between OpenAI and Fintech companies

Since its inception, a synergetic partnership between fintech companies and Open AI has existed. The partnership is quickly changing how financial operations are being executed. These Fintech companies are innovative entities now integrating OpenAI to expand the boundaries they can achieve in their financial operations. OpenAI has been used by fintech institutions in the following ways:

Spearheading Intelligent Investing

Key to this new advent is the growth of robo-advisors, whereby OpenAI's data-crunching abilities equip investors with algorithm-driven and personalized tips (P. Mahajanam 2023). The collaboration between OpenAI's analytical prowess and fintech's accessibility upscales intelligent investing, making intricate strategies accessible to vast audiences.

Using Blockchain to Revolutionize Transactions

Incorporating OpenAI into blockchain technology has revolutionized how transactions are carried out. OpenAI has advanced skills in understanding complex instructions and has helped streamline and secure agreements using smart contracts. The marriage has set the bar for a future controlled and managed by decentralized and transparent financial operations and increased its efficiency.

Enhancing Customer Experience

OpenAI has natural language processing techniques that improve customer interactions in fintech companies. Such natural language-reliant tools include chatbots and virtual assistants, which offer a personalized and seamless user experience when powered by OpenAI algorithms. These interfaces have redefined customer engagement by assisting in financial planning and answering queries and have made financial services approachable and user-friendly.

Fortifying Security Structures

OpenAI and fintech partnership extend to fraud prevention and risk management. Open AI has powerful algorithms that analyze existing patterns in real-time and identify anomalies and other likely frauds with utmost accuracy. This proactive measure protects financial institutions and revamps consumer trust by ensuring that the security and integrity of AI-powered financial services are upheld.

Manoeuvring Regulatory Practices

As the partnership transcends time, it becomes more essential to navigate regulatory landscapes. Fintech institutions, in collaboration with OpenAI, employ various strategies to comply with the set regulations. The two must balance innovation and concurrently adhere to changing legal frameworks to ensure they remain responsible and promote sustainable growth amongst themselves.

Financial Companies using OpenAI: The Case of Stripe and Mastercard

Stripe

One financial company that has harnessed Open AI's powers in fraud detection is the Irish/American financial services company Stripe. It is among the pioneering OpenAI's GPT-4 users. Stripe

facilitates the payment of large and small businesses over the Internet. As the organization develops its ecosystem to support all elements of the payment procedures, developers become their fundamental users. The more accomplished the developers grow while enrolling in Stripe, the more Stripe expands through the digital payments realm and grows the Internet's GDP.

The shift to OpenAI began when Stripe summoned a team of 100 staff from its different departments to cease their duties and brainstorm how GPT-4 would optimize old features or develop new ones for the organization. Stripe tasked the 100 employees with dreaming up functionality and features to use in the payment platform using OpenAI's language learning model's newest generation, GPT-4 (Boukherouaa et al. 2021). Stripe's specialists from the onboarding, support and risk sections considered where their institution would leverage artificial intelligence that comprehends free-form images and text and develops human-like responses to either change or improve workflows or features.

According to Eugene Mann, Stripe's Applied Machine Learning Team product lead, the company's mere access to GPT-4 helped them realize they had various problems that could be amicably solved using GPT. Mann stated that their primary mission was to discover workflows or products across the organization that would be enhanced using large language models and understand specific areas where the models would work well or struggle in delivering results. Stripe is a familiar user of AI as it used OpenAI's previous sequel technology, GPT-3, to aid its support team in better serving users through services like summarizing a user's query and routing issue tickets.

In the initial development process, Stripe's team assembled 50 potential applications to test GPT-4. After vigorous testing and vetting, 15 of the prototypes emerged as strong candidates that would be incorporated into the platform to serve functions that included fraud detection, support customization and answering any questions pertaining to support. Stripe uses OpenAI in the following operations;

Seeking Clarity over the Users' Operations

To enhance user experience and give the expected support, Stripe has to precisely understand how each of its customers uses the platform and tailor its support accordingly. Although it may seem like an obvious step, it needs long human hours to master and effect.

Mann states that most businesses, for instance, nightclubs, keep their websites mysterious and sparse, making it challenging as one searches to discover what is happening on such platforms. However, the advent of GPT-4 has enabled Stripe to scan such websites and provide a summary that vastly outdoes those performed using human skills. Upon hand-checking the results, Stripe realized that humans were wrong, but the model deployed was the right pick. However, GPT-4 has now erased any traces of uncertainty as it produces accurate results.

Answering Queries Regarding Documentation

Yet another way Stripe supports developers is through detailed technical documentation and a strong developer support team that answers technical queries or troubleshooting-related challenges. GPT-4 can understand, digest and provide virtual assistance. The technology understands all questions from the user and reads comprehensive documentation for them.

Detecting Fraud in Community Platforms

The need arises to control harmful or malicious actors. Stripe houses a strong community on forums such as Discord, which not only crowdsources help for niche technical queries but also enhances developers' visibility for upcoming works. However, since it operates online, malicious fraudsters gain access to such forums, mainly intending to access crucial information from community members or obtain credibility with Stripe's community team after being expelled from the platform.

GPT-4 becomes helpful in this scenario by evaluating the posts' syntax on Discord and flagging accounts where Stripe's fraud team should investigate and ascertain that it is not a fraudster in disguise. GPT-4 is also helpful in scanning inbound communications and discovering coordinated activities from suspected actors.

Future Engagements

The Stripe Team is now considering other upcoming features from OpenAI. GPT can be harnessed as a business coach that can interpret revenue models or advise financial institutions on effective strategies. As GPT grows more intelligent over time, its potential areas of applications keep growing.

MasterCard

Mastercard is another beneficiary of the new AI-powered tool in fighting financial fraud. Mastercard adopted the use of AI technology in the last decade. Today, AI has evolved into a foundational technology deployed all over Mastercard’s operations and has become a game-changer in identifying fraud patterns. The new AI-powered cybersecurity solutions have saved over $35 billion in fraud losses in the last three years [26]. It uses AI to help banks envisage upcoming frauds in real-time before any funds are transferred from a victim’s account. If all U.K banks successfully adopt the new technology, the Trustee Savings Bank predicts a decrease in scam losses of up to $100 million [26]. Ranging from simple enticing scams to fictitious online frauds, impersonation scams of various forms have hurt businesses and individuals over recent times and reduced the confidence of those yet to be scammed. However, the situation is changing as financial institutions like Mastercard have reinforced the fight against online fraudsters using a new Consumer Fraud Risk Solution.

By using the organization's new AI capabilities and its exemplary network monitoring of account-to-account payments, the new technology helps financial institutions look for any impending fraud. Mastercard has partnered with nine UK banks, including Bank of Scotland, TSB, Lloyds Banks, Monzo, Halifax and now uses large-scale payment data in picking out actual payment frauds before initiating a funds transfer from any account.

Organized fraudsters have scammed unsuspecting individuals through a series of assumed mule accounts by disguising them as trustworthy parties. To battle the trend, Mastercard collaborated with United Kingdom Banks to track the flow of funds through these fraud accounts and lock them out. Using insights gained from the tracking activity and supporting them with unique analysis factors like payment values, payee history, account names, payer details and payee's links to accounts linked with scams, Mastercard's AI tool gives banks the needed intelligence to intervene in real-time and thwart any suspicious payment in time. Trustee Savings Bank is among the first beneficiaries of the new revolution. The bank has adopted Mastercard's Consumer Fraud Risk Tool. In its first four months, the bank attests that the new tool has revamped its fraud detection capabilities. Based on its reports, in the U.K., the amounts that would have been saved from scams in a year is £100m [26], should all banks adopt the solution. Other banks have on-boarded the process and Mastercard looks to scale the solution to other international markets.

As payment and banking security advances, scammers have opted for impersonation tactics to bypass security measures. They aim to convince people or institutions to send them funds, thinking they are legitimate people or entities. Mostly referred to as APP (authorized push payment) fraud, it accounts for 40 % of the United Kingdom's bank fraud losses and it is predicted that it could cost $4.6 billion in the U.K. and U.S alone by 2026 [26]. Ajay Bhalla, Mastercard's president of Cyber and Intelligence admits that banks find these scams challenging to detect (Mastercard 2023). He states that customers bypass all set security checks and send the funds themselves, saving criminals the need to breach any security measures. Online fraud erodes customers' confidence in digital financing in a digitally advancing world. Bhalla reiterates that Mastercard's mission is to build and maintain customer trust. Using the new AI technology, Bhalla believes, will help banks identify and forecast any payments linked to fraudsters and stop them early enough.

TSB's director of Fraud Prevention, Paul Davis, compares identifying fraudulent payments among the millions of transactions carried out within a day to looking for a needle in a haystack. According to Paul, the new TSB's partnership with Mastercard will give the financial intelligence required to discover fraudulent accounts and deter any payments linked to such accounts.

Results generated from banks adopting Consumer Fraud Risk's score reveal massive success in preventing fraud, especially when deployed with various insights concerning customers and their

behaviours. This has helped the banks develop fraud strategies that precisely identify various forms of fraud, mainly romance, impersonation and purchase scams. Purchase scams are the leading firms in the U.K., accounting for 57 % of all scams and a significant nuisance for the banks 1. In 2022, the U.K experienced 207 372 cases of authorized push payment scams and incurred losses of up to £485 million [26].

OpenAI as an Advantage for Fraudsters

The scene has become two-way traffic as upcoming fraudsters can use OpenAI to stage unsuspected scams on innocent victims. Using OpenAI, scammers can imitate a person's voice and identity and carry out scams on their banking institutions. According to Soups Ranjan, CEO and co-founder of Sardine, a San Francisco-based fraud prevention startup, fraudsters now have access to flawless grammar, similar to a native speaker (Mastercard 2023). Banking customers are often falling victim to more swindles because they are now getting almost perfect disguising text messages.

In the new realm of generative AI, deep learning models can curate content based on the information they get trained on. It has therefore become easier for fraudsters to generate video, text or audio that can not only convince potential individual victims but also the programs or software intended to prevent the fraud. The same analogy has resurfaced with the advent of OpenAI. The fraudsters have been long adopters of new technologies as law enforcers struggle to cope. For instance, an article by Churbuck (D. Churbuck 1989) explains how thieves used laser printers and ordinary personal computers to excellently forge cheques to trick the banking institutions, which during those times, had lagged in establishing measures that would detect fake cheques.

Generative AI has grown threatening. It could sadly make high-tech fraud prevention technology, for example voice authentication, obsolete. According to a survey conducted by Deep Instinct (Deep Instincts 2023), a New York-based cyber firm, on 650 cybersecurity experts, three out of four sampled cybersecurity experts noted an upsurge in attacks the previous year. 85 % of the cybersecurity experts attributed the surge to online fraudsters leveraging generative AI. Customers, in 2022, reported losses amounting to $8.8 billion through online fraud, a 40 % increase from the previous year. This is according to a report obtained from the US Federal Trade Commission reports (J. Mayfield 2023). Massive monetary losses arise from online frauds, but imposter scams have taken centre stage as AI has bolstered them.

Fraudsters can harness generative AI capabilities in myriads of cunning ways. If a person often posts on online or social media platforms, the fraudsters can train an AI model to type in the person's style. They can also contact your relatives and implore them to send you funds. More astonishingly, fraudsters can use a short audio sample of a person's voice to convince relatives through impersonation. In extreme

cases, they stage kidnappings and ask for ridiculous ransom using the voice. Jennifer Destefano, an Arizonian mother of four, once faced such a predicament and later testified to Congress (U.S. Senate Committee on the Judiciary 2023). Not only are relatives being scammed, but businesses have fallen victim too. Fraudsters have disguised themselves as actual suppliers and crafted deceiving yet convincing emails to accountants claiming immediate payments. They proceed to attach payment instructions for bank accounts they can manipulate. Ranjan, Sardine's CEO, confirms that Sardine's fintech startup customers often fall prey to such scams and lose thousands of monies in such scams. These amounts may seem little compared to the $35 million a Japanese company lost in 2020 after one of its directors' voices was cloned and later used to stage an intricate swindle (T. Brewster 2021). That was a prelude to what was to follow, as AI capabilities now spill to video manipulation, writing and voice impersonation services. These AI tools have become cheaper and more accessible to fraudsters. Much earlier, one needed hundreds or perhaps thousands of photos to curate a high-quality, deep fake video. However, AI can now complete such tasks using a few photos.

As financial institutions adapt AI to curb fraud, online crooks are updated on the same as they develop off-the-shelf tools. This has seen the emergence of names like WormGPT and FraudGPT, reliant on generative AI models used by tech corporations with fraud intents.

In one fake YouTube video, generative AI helped clone Elon Musk’s voice and face hawking a crypto investment prospect that involved a $100,000,000 Tesla-sponsored bargain, which promised to give back double the bitcoin, dogecoin, ether or tether amount the investors would pledge. In the video, Elon was heard appreciating the interested investors and hailed the platform as an online broadcast enabling all cryptocurrency owners to increase their incomes. In this low-resolution video, Musk attributed the lack of clarity to hosting the crypto event from SpaceX. Since the video was fake, innocent and unsuspecting investors would have fallen victim to this scam. Scammers had used a similar 2022 YouTube Video (CNET 2022) he had given while on a SpaceX spacecraft program and impersonated his voice and image. Although YouTube pulled the fake video down, any investor that had sent crypto to any of the issued addresses lost their funds to innovative fraudsters that harnessed the power of generative AI. Musk remains a significant target for impersonations, as numerous audio samples are online to power AI-enabled voice clones. However, these fraudsters can impersonate almost anyone with online audio samples.

Voice impersonations are also gaining much use in scamming people through calls. The elderly American population is mainly targeted in this case. Everyone needs to be cautious about incoming calls, even when they are from what seems to be conversant numbers. Victims who have once been scammed find it challenging to trust any incoming calls due to spoofing phone numbers in robocalls, according to Kathy Stokes, director of fraud prevention programs at AARP, a lobbying and services provider with more

than 38 million members aged over 50 years (Mastercard 2023). Stokes claims they always suspect emails and text messages sent to them, which has posed severe concerns for their primary communication channels.

Another worrying development is the new threat to the already established security structures. For instance, Vanguard Group is a huge financial institution that has given voice recognition utmost priority to its customers. This mutual fund giant serves over 50 million investors and allows its clients to access specific services over the phone by speaking instead of answering security questions. Vanguard Group entrusts the client's voice to be as unique as their fingerprints, according to its 2021 video promotion on YouTube (CNET 2022). The company was rallying its members to sign up for its voice recognition feature in the video promotion. However, the latest exploits in voice-cloning suggest that financial institutions should rethink such practices. Ranjan, Sardine's CEO, claims that she has seen individuals deploying voice cloning to authenticate with unsuspecting banks and. access accounts effortlessly (Mastercard 2023).

Large and small businesses that use informal procedures to pay bills or transfer funds are also critical targets for online AI fraudsters. Since time immemorial, fraudsters have been emailing fake invoices to demand payment bills that appear to have been initiated by suppliers. The practice can reach higher levels of deceit as fraudsters can use the AI tools to call the company's employees using cloned versions of the executive's voice and order transactions or ask employees for sensitive information to conduct vishing or voice vishing attacks. According to Rick Song, CEO at Persona, impersonating an executive for highly valued fraud remains one of the biggest fears of voice recognition security measures (Mastercard 2023).

Criminals continuously use generative AI to engage fraud-prevention specialists assigned to thwart these threats in the digital finance system. Fraud prevention specialists must verify that the customers are who they claim to be to safeguard the institution and the customers from losses from online fraud. One of the ways that fraud-prevention businesses like MiTek, Socure and Onfido verify their users is by use of liveness checks. This method requires the user to take a video or selfie photo and the fraud prevention specialists use the elements to match the live face with the face found in the ID, which the user is also prompted to submit. When they understand how the system operates, online fraudsters purchase images of driver's licenses on the dark web and use the now cheaper and available video morphing programs to superimpose the real faces onto theirs. The program also allows them to talk and move their heads behind real people's digital faces, maximizing the chances to bypass the liveness checks.

There has been an upsurge in the generation of fake faces. The fake faces are high-quality and used to mount automated attacks to impersonate liveness checks. The upsurge varies according to the industries, but the previous years have recorded significant cases. Crypto and Fintech companies have experienced the highest number of impersonated liveness check attacks. Fraud experts reported to Forbes that they suspected

that well-established verification providers such as MiTek and Socure have experienced their fraud prevention metrics degrade due to the attacks. Johnny Ayers, Socure's CEO, points out that some clients need to be more active in adopting the firm's new models, which could adversely affect their performance (Mastercard 2023). Ayers also pointed out a top bank behind four versions, citing the dangers posed to the financial institution.

MiTek failed to comment on its performance metrics. However, Chris Briggs, its senior vice president, claims that if a particular model were developed some months ago, it would be argued that the older model performed at lower levels than the newer models. The vice president stated that the firm's models undergo vigorous training and retraining trained and retrained using lab-based and real-life data streams.

Wells Fargo, Bank of America and JPMorgan failed to remark on the impediments they faced with generative AI-powered online scam. One spokesperson from Chime, America’s most prominent digital bank and a victim of significant fraud problems, also claims that the institution has not recognized any upsurge in generative AI-powered fraud attempts (Vanguard 2021).

Online fraudsters behind the growing financial scams vary from solo individuals to well-organized groups made of hundreds of tech gurus. The organized online groups work in multi-layered structures and have adept members, with data scientists onboard. They own their command-and-control centers. Some members are only tasked to identify leads by phishing phone calls and emails. When their phishing attacks get an unsuspecting customer, they hand them over to the next colleague in line, who masquerades as a bank branch manager and attempts to persuade the victim to transfer the money from the account. One of the critical steps in the scamming process involves persuading the victim to install a program like Citrix or Microsoft TeamViewer that allows them to control their computer. With such levels of control on the victim's computer, the online fraudsters further stretch to carrying out more purchases and withdrawing funds to other addresses.

OpenAI has attempted to develop precautions that hamper people from using ChatGPT to commit fraud. For example, the model immediately declines any attempt to initiate ChatGPT to ask an individual for their account number. OpenAI recognizes fraudsters' possible misuse of the platform and has a safety and misuse policy on its website that reads. There is no silver bullet for responsible deployment, so we try to learn about and address our models' limitations and potential avenues for misuse at every development and deployment stage." (Haverstock and Kauflin 2021).

Meta, on the other hand, released a language model, Llama 2, which is even easier to use for advanced criminals due to its open-source nature, which displays all its deployed codes. This expands the possible number of ways online fraudsters can tailor it to their advantage and spell doom on unsuspecting

victims. These fraudsters can develop malicious AI tools on top of the model. Amid the insecurity concerns, Meta CEO Mark Zuckerberg said Llama is open-sourced to enhance its security and safety. According to Zuckerberg, many people can scrutinize open-sourced software to highlight and fix issues.

Fraud prevention organizations are rapidly trying to innovate and remain updated by increasingly assessing new data types to identify possible fraudsters. Defining people as being who they are online is a challenging feat to achieve and calls for the use of AI. AI will be needed to combat the generative AI-powered trickery from the fraudsters.

Summary

OpenAI is a revolutionary tool in finance. However, its usefulness will depend on the parties being more conversant and updated about leveraging its powerful tools. Its deep machine learning tools are used in the financial sector in various operations, including using blockchain to revolutionize transactions and chatbots to enhance customer experience. Machine learning has also been a cheat code in fraud detection, as financial fraud detectors harness the power of neural networks, decision trees, algorithms, natural language processing and machine learning to develop robust security structures that thwart fraud attempts. International companies like Stripe and Mastercard can attest to the benefits of using OpenAI in detecting fraud and they hope to upscale their AI operations into their business. However, if OpenAI lands in the wrong hands, it can be used to swindle money from these financial institutions effortlessly, as depicted by the emergence of the terms WormGPT and FraudGPT. Numerous cases have been reported involving use of generative AI to clone voices and images or even generate convincing texts that con unsuspecting individuals or organizations. Since fraudsters will always be on the move to curb their economic needs, fraud detection specialists must proactively use OpenAI to curb these attacks and protect their financial institutions from incurring huge losses through online fraud.

References

[1]. Colvin, G. (2020, November 12). *The pandemic may be the greatest environment for business fraud in decades*. Fortune. https://fortune.com/2020/11/12/pandemic-corporate-fraud-scams/

[2]. Littman, A. (2011). *The Fraud Triangle: Fraudulent Executives, Complicit Auditors and Intolerable Public Injury*. CreateSpace Independent Publishing Platform.

[3]. Ciobanu, M. (2020, March 12). *Why understanding your fraud false-positive rate is key to growing your business*. The Paypers. https://thepaypers.com/thought-leader-insights/why-understanding-your-fraud-false-positive-rate-is-key-to-growing-your-business--1241130

[4]. Mullen, C. (2023, January 5). *Card industry's fraud-fighting efforts pay off: Nilson Report*. Payments Dive. https://www.paymentsdive.com/news/card-industry-fraud-fighting-efforts-pay-off-nilson-report-credit-debit/639675/

[5]. Pascual, Marchini, & Miller. (2017). *Identity Fraud: Securing the Connected Life*. Javelin Strategy. https://javelinstrategy.com/research/2017-identity-fraud-securing-connected-life

[6]. Sando, S. (2021). *Consumer Preference Drives Shift in Authentication*. Javelin Strategy. https://www.javelinstrategy.com/coverage-area/consumer-preference-drives-shift-authentication

[7]. Villalobos, M. A., & Silva, E. (2017). *A Statistical and Machine Learning Model to Detect Money Laundering: An application*. http://hddavii.eventos.cimat.mx/sites/hddavii/files/Miguel_Villalobos.pdf

[8]. Awoyemi, et al. (2017). *Credit card fraud detection using machine learning techniques: A comparative analysis*. In 2017 International Conference on Computing Networking and Informatics (ICCNI). IEEE.

[9]. Herland, M., Khoshgoftaar, T., & Bauder, R. (2018). *Big data fraud detection using multiple Medicare data sources*. Journal of Big Data, 5(1), 1-21.

[10]. Ayyadevara, V. (2018). *Pro machine learning algorithms*. Apress.

[11]. Graupe, D. (2016). *Deep Learning Neural Networks*. World Scientific Publishing Company.

[12]. Mahajanam, P. (2023, March 6). *How AI is revolutionizing fraud detection in financial transactions and processes*. Times of India. https://timesofindia.indiatimes.com/blogs/voices/how-ai-is-revolutionizing-fraud-detection-in-financial-transactions-and-processes/

[13]. Boukherouaa, E. B., et al. (2021). *Powering the Digital Economy: Opportunities and Risks of Artificial Intelligence in Finance*. International Monetary Fund.

[14]. OpenAI. (2023, March). *Stripe leverages GPT-4 to streamline user experience and combat fraud*. https://openai.com/customer-stories/stripe

[15]. Mastercard. (2023, July 6). *Mastercard leverages its AI capabilities to fight real-time payment scams*. https://www.mastercard.com/news/press/2023/july/mastercard-leverages-its-ai-capabilities-to-fight-real-time-payment-scams/

[16]. Churbuck, D. (1989). *Desktop Forgery*. https://churbuck.com/wp-content/uploads/2014/01/desktopforgery.pdf

[17]. Deep Instincts. (2023). *Generative AI and Cybersecurity: Bright Future or Business Battleground?* https://www.deepinstinct.com/voice-of-secops-reports

[18]. Mayfield, J. (2023, February 23). *New FTC Data Show Consumers Reported Losing Nearly $8.8 Billion to Scams in 2022*. Federal Trade Commission. https://www.ftc.gov/news-

events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022

[19]. U.S. Senate Committee on the Judiciary. (2023). *Artificial Intelligence and Human Rights*. https://www.judiciary.senate.gov/committee-activity/hearings/artificial-intelligence-and-human-rights

[20]. Brewster, T. (2021, October 14). *Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find*. Forbes. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=3b7b78247559

[21]. CNET Highlights. (2022). *WATCH: Elon Musk's SpaceX Starship Update Event - Livestream*. https://www.youtube.com/watch?v=MpTLExoMAtQ

[22]. Vanguard. (2021). *How voice verification works*. https://www.youtube.com/watch?v=UQIwLZQruLE

[23]. Haverstock, E., & Kauflin, J. (2021, December 3). *Fintech's Fraud Problem: Why Some Merchants Are Shunning Digital Bank Cards*. Forbes. https://www.forbes.com/sites/elizahaverstock/2021/12/03/fintechs-fraud-problem-why-some-merchants-are-shunning-digital-bank-cards/?sh=61bb7c4375bd

[24]. OpenAI. (2022, March 3). *Lessons learned on language model safety and misuse*. https://openai.com/blog/lessons-learned-on-language-model-safety-and-misuse/