**A04 AI in Fraud Detection Case Studies**

**Introduction**

Every year, banks and other financial institutions lose billions of dollars due to fraud and malpractice. With not just the financial loss hitting the banks, customers lose trust and faith within businesses whenever it’s not properly handled or prevented. When the Covid pandemic hit in 2020, online businesses and transactions became much more common, as well as fraud from phishing, and online attacks/breaches due to more people placing their money in digital banks.

This is especially dangerous with the growing presence of AI, new models and tools are able to adapt and steal information better than ever, and it’s important for banks to use their own AI tools to adapt and prevent further losses for their customers down the line.



**JP Morgan Chase Bank**

**Introduction**

J.P Morgan is the largest bank within the United States, and leads in banking investments, commercial banking, asset management, and transaction processing. Being the largest bank in the US, they handle millions of transactions and fraud reports every year and with how many assets they’re handling, security and early prevention is more important than most financial institutions out there. AI shows the capability to cut costs, boost productivity, increase efficiency, and predict fraud trends to prevent them early on.

**Technology Overview**

One way JP Morgan prevents fraud is utilizing Large Language Models (LLMs) trained on fraudulent emails, texts, messages, and situations to recognize terms and phrases used to extract information. Phishing for account details is one of the most common ways people are scammed and can be difficult to detect for people tricked into believing unofficial messages are real. Using these AI models, they can automatically be flagged and stopped in place before any information or data is stolen.

Sample Data Trends: ([Payments data for Fraud Detection](https://www.jpmorgan.com/technology/artificial-intelligence/initiatives/synthetic-data/payments-data-for-fraud-detection))

A table with numbers and letters

AI-generated content may be incorrect.

Generative AI as a whole also can be trained off entire trends of fraud, and personalized data per customer to detect anomalies or irregularities within spending patterns. Since AI is able to access and read entire databases in seconds, they work far more efficiently at stopping any scams before they even happen.

**Benefits**

JP Morgan has shown to have increased fraud detection up to 25% more and cut false positives down by 20%. With more successful transactions and less false flags, efficiency of payments and overall growth is easier, while stopping fraud more successfully also reduces losses from compromised accounts. This is all done without the use of manual review either, meaning that these tasks can be fully automated and done around the clock without the need for a worker so all times of the day/night transactions can be handled easily.

**Challenges**

One of the main challenges when it comes to AI with JP Morgan is bias, and ethical concerns as a whole. Since loans and investment predictions may be based on bias depending on the individual using them, it may lead to improper outcomes when trying to properly predict the best course of action for a customer. There’s also the concern of jobs being replaced or lost since AI can completely replace teams dedicated to preventing and detecting fraud, predicting potential investments, and more since it’d be more efficient and cheaper to not pay for employee wages and benefits.

**Conclusion**

JP Morgan’s use of AI shows great potential for security and growth, although it shows potential to breach personal data and make unfair bias based off it. Since AI models aren’t perfect, there still needs to be human working and intervention as an alternative method, but I think the best place for AI would be in preventing fraud since the main ethical concern is stopping a human worker from doing it instead. When it comes to detecting fraud, if the AI messes up due to bias the worst case is that they might need to manually confirm a transaction, instead of something like a loan being outright rejected due to unfair bias.



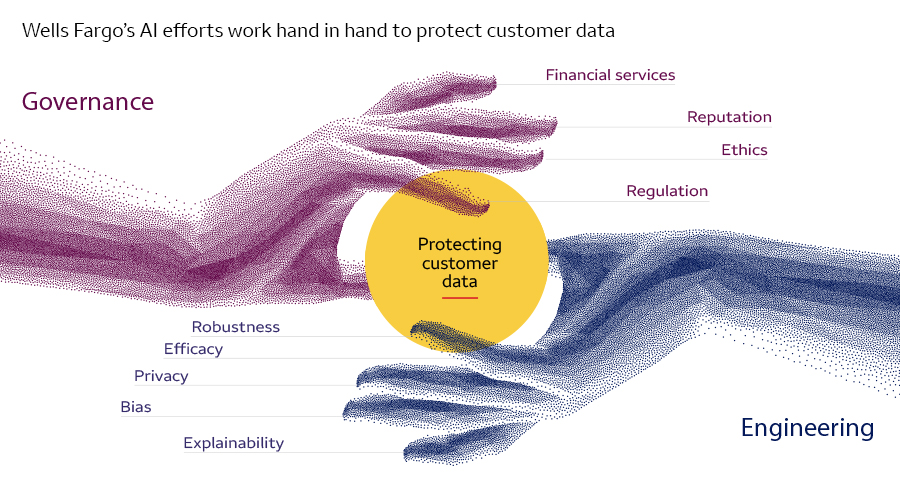
**Wells Fargo**

**Introduction**

Wells Fargo is one of the biggest US-Based banking services, providing investment, credit card, loan, and account services to its customers. Wells Fargo has mentioned interest in implementing AI for a while, stating its capabilities to personalize experiences, speed up loan applications, and improve fraud detection. Specifically Wells Fargo shows interest in generative AI and making sure that it can be trained to be “responsible” and ethical in its use.

**Technology Overview**

Wells Fargo has stated four main points to follow when developing their AI, beating bias, No rogue AI, alternative options, and partnership/research. Teams have been assigned to manually validate data and test them for potential biases as well as added transparency so it’s easy to understand how and why AI provides the output it does through open-source platforms. They’ve stated this completely prevents the AI from “hallucinations” which make up random facts and data, which may cause critical issues within a banking corporation.



[How Wells Fargo builds responsible artificial intelligence](https://stories.wf.com/how-wells-fargo-builds-responsible-artificial-intelligence/)

**Benefits**

Wells Fargo has stated that AI will completely revolutionize the banking industry as a whole, with all new ways of detecting fraud, assisting clients and bankers, and making sensible decisions off trends. This can save billions of dollars for them, and make many mundane or simplistic tasks completely automated, saving time and making the workflow more efficient. Personalized banking will also provide customers with better options based on their habits and situations, handling data and decisions far better than humans would be able to manually find.

**Challenges**

As they’ve stated in their points to develop AI, it’s important to make sure they remove bias and provide transparency. Wells Fargo tries to avoid ethical issues by working with others and building their AI around working with people rather than completely replacing them. Completely removing bias with a predictive AI trying to guess demographics and trends is incredibly difficult and will inevitably make some mistakes if any remaining bias is undetected on finished models.

**Conclusion**

Wells Fargo hasn’t fully released or implemented their AI systems beyond basic detection improvements and personalization plans. They’ve shown interest in building a fully responsible model to work alongside people ethically and efficiently, although this takes much more time, effort, and money compared to traditional training models. The full view of their finished AI will be able to fully make decisions for loans, flagging, and customer interests all on their own.



**PayPal**

**Introduction**

PayPal is an online financial institution focused on processing payments online. It allows you to link your bank and prevent needing to enter in detail on websites which reduces the risk of information getting stolen. With a service based around security, it’s especially important to recognize when an account may be compromised since payments can easily get allowed without the bank batting an eye since PayPal would be considered a trusted service.

**Technology Overview**

PayPal initially tested building models for fraud detection and compromised accounts on CPU servers, which weren’t able to handle their needs of operating around the globe at all times. Switching over to NVIDIA’s T4 GPUs PayPal was able to massively improve their performance, the server load was reduced by nearly 8x, while their fraud detection systems were improved by 10%. PayPal also uses AI for improving commerce and payment offerings tailored to customers and merchants personally, allowing real time assistance and updates without the need for human intervention.

**Benefits**

As stated in the technology overview, PayPal was able to improve their detection rates by 10% and personally tailor their services to each customer and business personally. This heavily improves the quality of service that PayPal is able to provide, using predictions based off individual payment trends allows even non-suspicious fraudulent activity to be detected early on. Since they work globally, utilizing AI allows their service to work at all times around the world with assistance since AI doesn’t need breaks or sleep schedules changing based off time zones.

**Challenges**

PayPal actually has less challenges when it comes to implementing AI systems considering a majority of their services are online and server-based. Implementing AI doesn’t mess with physical workflow as much as a normal financial institution and can work seamlessly with the services that already exist rather than replacing certain positions.

**Conclusion**

PayPal is an online based payment processor that has utilized AI to improve its fraud detection, commerce, and recommendations based on personal data. Their model structure uses NVIDIA GPUs trained on transactions, and fraud patterns within a neural network.



**American Express**

**Introduction**

American Express is a financial institution that offers banking services, and various types of credit cards. They’re also one of the top issuers of personal and business credit cards by handling over eight billion transactions annually. American Express is affected by scams and fraud since they can cause customers to lose lots of cash and assets if activity isn’t detected and prevented early on, but with their billions of transactions going through their services every year it can be difficult to actively monitor and prevent fraud from occurring.

With the use of AI, every transaction can be monitored and tracked in real time and give a smarter response to prevent potential fraud from happening.

**Technology Overview**

American Express worked with deploying deep learning models running on NVIDIA’s Triton Inference Server, which are trained on NVIDIA DGX, and then further optimized by NVIDIA TensorRT. The Triton Inference Server makes wide-scale model deployment simple, and the TensorRT helps minimize latency while maximizing throughput within trained models. NVIDIA stating that their system had a 50x improvement over a CPU-Based configuration which couldn’t handle the needs of American Express.

The model is a real-time fraud detection system, based on a “GPU-accelerated LSTM deep neural network, combined with a gradient boosting machine (GBM).”. The model analyzes various types of information including spending patterns, locations, and personal information to determine whether a transaction may be fraudulent.

**Benefits**

Utilizing AI has reduced the need for manual review and flagging of transactions, as well as the accuracy of fraudulent transactions detected. Instead of only certain transactions being flagged on basic reasoning, AI can use advanced personal knowledge of spending habits to determine whether activity is suspicious or not and pause/flag the alert for further review.

**Challenges**

American Express hasn’t stated any issues with implementing their model, besides having to improve from a CPU-based model that wasn’t powerful enough. AI being implemented to prevent fraud has only increased their accuracy and detection rate, preventive losses being able to mitigate the cost of any implementation of their AI.

**Conclusion**

American Express is one of the largest credit card distributors in America with billions of transactions happening every year. By teaming up with NVIDIA’s AI services, they’ve been able to implement a GPU-based deep learning model for real time fraud detection. By Implementing AI, they’ve successfully increased the rate of fraud detected and stopped by using smart reasoning based off spending data.



**Swedbank**

**Introduction**

Swedbank is one of Sweden’s largest banks, offering accounts, financial advice, loans, investments, and promotes financial education. Swedbank was victim of a massive money laundering scandal from their former CEO, which decreased their stock price in 2018 – 2019 by over 30%. As a response to this, Swedbank has worked on developing AI to detect both fraudulent transactions, and money laundering for early prevention.

**Technology Overview**

A graph with a red line and blue line

AI-generated content may be incorrect.Swedbank used multiple NVIDIA GPUs in parallel to train multiple generative adversarial neural networks (GANs) trained to detect anomalies in spending, and better tracking of transactions/finances. Using NVIDIA’s GPUs and Triton Framework, their GANs models were trained on NVIDIA’s DGX systems on a multi-node framework which massively increased the number of samples generated per GPU added.

**(**[**Detecting Financial Fraud Using GANs at Swedbank with Hopsworks and NVIDIA GPUs | NVIDIA Technical Blog**](https://developer.nvidia.com/blog/detecting-financial-fraud-using-gans-at-swedbank-with-hopsworks-and-gpus/)**)**

**Benefits**

Swedbank hasn’t released exact details of how effective their AI implementation was, but NVIDIA, whose resources were used by Swedbank stated that similar financial institutions have actively saved over $100 million a year through AI fraud detection. Using these models, Swedbank can also keep their own assets in check through their anti-laundering detection, their work to prevent money laundering is important to rebuilding trust with their customers. Prioritizing their AI towards money laundering is great for that goal of rebuilding trust, as well as saving them from future incidents.

**Challenges**

The main challenge related to building and implementing their AI was having to add the additional focus on stopping money-laundering. With how much the company lost due to problems with it in the past, it was necessary to build these features into the AI to prevent it and rebuild their reputation. Although other financial institutions have developed their AI to detect and prevent fraud, they had to develop more unique methods to dedicate a portion of it to Anti-Money Laundering features.

**Conclusion**

Swedbank is one of the largest banks within Sweden and has faced problems with fraud and money laundering which cost them a big portion of their stock. Utilizing NVIDIA’s frameworks, they developed GANs models to detect fraud and prevent money laundering in the future. These developments have the potential to both save them millions of dollars annually and rebuild their reputation after their previous money laundering scandals.

**BNY Mellon**

**Introduction**

BNY is one of the oldest banks in America but also provides its services to over 30 countries in the world. It offers large investment services, having access to around 20% of the global investable assets. BNY controls over 50$ trillion in assets, their customer base going from personal accounts all the way to businesses and corporations, meaning security is very important to maintain. AI doesn’t just allow BNY to monitor fraudulent charges and activity better, but also provide personal planning, and market prediction/trading algorithms.

**Technology Overview** Sources: BNY Advisors, U.S. Census Bureau.A screenshot of a graph

AI-generated content may be incorrect.

BNY monitored and gathered information on the use cases of AI within certain types of businesses and based their own on “reusable capabilities”. Their AI was named Eliza based off their founder Alexander Hamilton’s wife and teamed up with NVIDIA’s DGX SuperPOD and their Triton Inference Servers to create an AI “Supercomputer”. The AI is capable of predicting market trends, fraud detection, service automation, trade analytics, and more.

**Benefits**

The Benefits of Eliza AI has given many benefits to BNY, starting with their optimization of workflows and automation of tasks improving their productivity up by 40%. AI has also improved their products and overall business model by using personalized and smarter data and predictions for improved profits and customer satisfaction. The last report mentioned that BNY also managed to improve their fraud detection by 20% since the implementation of their new system.

**Challenges**

BNY has stated that every one of their employees should be able to utilize the AI itself, rather to “empower” them instead of replacing them. Focusing on using their AI to get rid of mundane tasks and encourage growth by giving their employees access to Eliza has gotten rid of many ethical concerns generated typically by AI. Although implementing AI alongside a normal workforce brings its own challenges, as Eliza may not be able to use its full capabilities since it’s being developed to be worked with, rather than on its own.

**Conclusion**

BNY is a large financial service company with connections to over 30 countries, and 20% of investable stocks within the world. Their AI Model, Eliza, was built with multiple re-usable capabilities based on AI use trends within other companies. Eliza has streamlined and improved many of BNY’s services and predictions and was specifically designed to be used and improve the efficiency of employees rather than replace them outright.

A red and orange circles

AI-generated content may be incorrect.**MasterCard**

**Introduction**

Mastercard is a financial institution focused mainly on making secure payment transactions. Fraudulent practices can lead to the core of MasterCard’s business being impacted, since there are many methods like spyware, skimming, phishing, or stolen numbers on their cards to get access to their account. Without proper safety measures, if stolen cards are able to successfully make transactions even on suspicious terms, then their customers may lose trust within MasterCard as a whole.

Using AI can minimize the damage to these frauds with early detection, or process reports of stolen information and take proper precautions earlier than a human employee would.

**Technology Overview**

For the specific technology Mastercard uses, they haven’t released details or a name for their fraud detection. Besides using amazon’s AWS AI and ML tools, they have only stated that they use a combination of different generative AI, and graph technology. They use data based on suspected merchants, previously reported frauds, and authorized transactions to detect patterns for potential scams, or other fraudulent activity to be flagged instantly. Meanwhile Graph technology allows them to track activity all across MasterCard’s network and are able to link and map together hundreds of cards and transactions together at once. They also use algorithms to detect specifically MasterCard numbers on illegal websites selling information, and prevent “BIN” attacks that use automated combinations to brute force their way in.

**Benefits**

From the benefits they’ve stated the detection of fraud and suspicious activity has gone up three times, while the number of false detections has gone down around ten times. This has also increased the rates of stolen or compromised cards being detected, as well as how fast fraudulent merchants are identified. This also reduces the need for manual review and study of many of these transactions, saving the company time and money. MasterCard has also reported that billions of dollars have been saved for providers and other merchants by making sure transactions run smoothly.

**Challenges**

The main challenge MasterCard faces is mainly the cost and replacement of workers with their AI. MasterCard has faced layoffs due to financial costs of implementing and developing AI to work within their network, since it requires a massive overhaul of many of their older systems. This also removed the need for certain positions and jobs that their AI can take over, many working to detect fraud, or work with managing credit card lines aren’t needed or wanted since developing an AI tool reduces the need for wage costs, time schedules, and benefits for employees.

This leads to the ethical question of how AI can create a lack of jobs for a certain field, although it’s more of a trade. In trade for more efficient detection systems, customers, merchants, and investors will be happier working with MasterCard to handle payments, but the employees working there themselves are put at risk of being unable to keep their job position.

**Conclusion**

In conclusion, MasterCard’s use of AI has greatly improved their fraud detection and saved billions of dollars for merchants and customers alike. They haven’t seemed to face any challenges with the AI itself, rather its implementation and power to reduce available jobs within the company. I think it’s important for companies to secure their data, and not avoid implementing AI just for employee benefit, but also not outright cut their job. Human interaction and assistance are important for many people, and the company itself in case of any system failures. Working within these AI-driven departments to assign alternate jobs or keeping them split between positions with less workload would be healthy for the work environment.

**Conclusion**

These case studies made me realize how important ethics come into the implementation of AI in these businesses. Although AI cut costs, improve performance, and seem like much better options for learning and predicting trends, the impacts it can have on people can lead to unfortunate situations. AI bias can give bad predictions or outputs based on people’s personal data, and AI can also take away certain job uses which can end up with people getting fired.

I think the best cases for AI are improving security and preventing fraud, as bias can actually be helpful when it’s tailored to what a person usually does with their spending habits. Meanwhile if AI is put into place to fully make decisions like who should get loans or benefits, as well as giving advice by itself it can lead to situations where customers and people end up getting negatively impacted.

**References**

Levitt, K. (2024, December 5). *How is AI used in fraud detection?*. NVIDIA Blog. https://blogs.nvidia.com/blog/ai-fraud-detection-rapids-triton-tensorrt-nemo/

**JP MORGAN CHASE BANK**

*About Us*. About us. (n.d.). https://www.jpmorgan.com/about-us

J.P. Morgan. (2023, November 20). *Ai Boosting Payments Efficiency & cutting fraud: J.P. Morgan*. AI Boosting Payments Efficiency & Cutting Fraud | J.P. Morgan. <https://www.jpmorgan.com/insights/payments/payments-optimization/ai-payments-efficiency-fraud-reduction>

*Payments data for fraud detection*. Payments data for Fraud Detection. (n.d.). https://www.jpmorgan.com/technology/artificial-intelligence/initiatives/synthetic-data/payments-data-for-fraud-detection

**WELLS FARGO**

About Wells Fargo. (n.d.). <https://www.wellsfargo.com/about/>

Hasty, C. (2024, October 8). *How AI can shape the future of banking*. Wells Fargo Stories. https://stories.wf.com/artificial-intelligence-has-the-potential-to-reshape-banking/

Frers, C. (2024, October 1). *How Wells Fargo Builds Responsible Artificial Intelligence*. Wells Fargo Stories. https://stories.wf.com/how-wells-fargo-builds-responsible-artificial-intelligence/

**PAYPAL**

*GPU inference momentum continues to build*. NVIDIA Technical Blog. (2023b, December 15). https://developer.nvidia.com/blog/gpu-inference-momentum-continues-to-build/

PayPal. (2024, November 6). *Machine Learning Fraud Detection Technologies*. Machine Learning Fraud Detection Technologies | PayPal US. https://www.paypal.com/us/brc/article/payment-fraud-detection-machine-learning

**AMERICAN EXPRESS**

Ashley, J. (2022, April 28). *American Express adopts Nvidia AI to help prevent fraud and foil cybercrime*. NVIDIA Blog. https://blogs.nvidia.com/blog/american-express-nvidia-ai/

[https://americanexpress.com/](https://americanexpress.com/American Express prevents fraud and foils cybercrime with Nvidia AI Solutions. NVIDIA Insights. (n.d.). https://www.nvidia.com/en-us/case-studies/american-express-prevents-fraud-and-foils-cybercrime-with-nvidia-ai-solutions/ )*[American Express prevents fraud and foils cybercrime with Nvidia AI Solutions](https://americanexpress.com/American Express prevents fraud and foils cybercrime with Nvidia AI Solutions. NVIDIA Insights. (n.d.). https://www.nvidia.com/en-us/case-studies/american-express-prevents-fraud-and-foils-cybercrime-with-nvidia-ai-solutions/ )*[. NVIDIA Insights. (n.d.). https://www.nvidia.com/en-us/case-studies/american-express-prevents-fraud-and-foils-cybercrime-with-nvidia-ai-solutions/](https://americanexpress.com/American Express prevents fraud and foils cybercrime with Nvidia AI Solutions. NVIDIA Insights. (n.d.). https://www.nvidia.com/en-us/case-studies/american-express-prevents-fraud-and-foils-cybercrime-with-nvidia-ai-solutions/ )

**SWEDBANK**

[Swedbank Group | Swedbank](https://www.swedbank.com/)

*Detecting financial fraud using Gans at Swedbank with Hopsworks and Nvidia gpus*. NVIDIA Technical Blog. (2023, January 13). https://developer.nvidia.com/blog/detecting-financial-fraud-using-gans-at-swedbank-with-hopsworks-and-gpus/

Geijer, M., & Deminor. (n.d.). *The case of Swedbank’s former CEO Birgitte Bonnesen: Landmark ruling for the Swedish banking sector and the future communication of publicly listed companies*. deminor. https://www.deminor.com/en/news-insights/the-case-of-swedbanks-former-ceo-birgitte-bonnesen-landmark-ruling-for-the-swedish-banking-sector-and-the-future-communication-of-publicly-listed-companies

**BNY MELLON**

*Unlocking AI growth in financial services*. BNY. (n.d.). https://www.bny.com/corporate/global/en/insights/unlocking-the-ai-growth-multiplier.html

*BNY Mellon, First Global Bank to deploy AI supercomputer powered by Nvidia DGX superpod with DGX H100*. NVIDIA. (n.d.). https://resources.nvidia.com/en-us-financial-services-industry/bny-mellon-superpod

**MASTERCARD**

Stripe. (2025, January 23). *What is MasterCard? A guide to the card network*. Stripe. https://stripe.com/in/resources/more/what-is-mastercard

Cuttler, E. (2024, November 2). *Inside the algorithm: How gen ai and Graph Technology are cracking down on Card Sharks*. Fraud detection using AI: Inside the algorithm | Mastercard Newsroom. https://www.mastercard.com/news/perspectives/2024/inside-the-algorithm-how-gen-ai-and-graph-technology-are-cracking-down-on-card-sharks/

Using AWS AI and ML services to detect and prevent fraud | Mastercard video | AWS. (n.d.). https://aws.amazon.com/solutions/case-studies/mastercard-ai-ml-testimonial/

Editore, G. (n.d.). How AI issues are impacting jobs at MasterCard (USA). https://www.reviewofailaw.com/Tool/Evidenza/Single/view\_html?id\_evidenza=1123