Artificial Intelligence Fraud Detection Case Study: Danske Bank

Hashim Sayed Hoosini

Houston Community College

A04_Hashim Sayed Hoosini_ ITAI 2372

Professor Sitaram Ayyagari

June 30, 2025

Artificial Intelligence Fraud Detection Case Study: Danske Bank

Abstract

Danske Bank, a leading financial institution in Denmark, faced increasing challenges from rising online fraud incidents. Their legacy rule-based fraud detection system flagged over 1,200 non-fraudulent transactions each day while failing to catch nearly 60% of actual fraud. Danske Bank turned to advanced artificial intelligence (AI) and deep learning to improve how effectively they detect fraud and to streamline their operations. This case study explores the specific AI tools they put in place, the advantages they gained, and the challenges they encountered along the way. It offers a real-world insight into how AI is being used to tackle fraud in the financial industry.

Danske Bank worked with a data science company, Think Big Analytics, to improve the way they detect fraud. Their goal was to move away from old-fashioned rule-based systems that often gave false alarms or missed real fraud. Instead, they introduced a smarter approach using deep learning of artificial intelligence (AI) that can learn from large amounts of data and spot patterns that humans or basic systems might miss. They trained an AI system using huge amounts of transaction data, such as when and where people use ATMs, make online payments, or use mobile banking apps. with understanding what normal behavior looks like for each customer, the AI can recognize when something seems off — like a sudden large transaction from a new location — and raise a flag. To make this system even more effective, Danske Bank used powerful computers with special graphics processing units (GPUs) that help the AI process information very quickly. This means the bank can spot and stop suspicious transactions almost in real time. One of the most interesting things they did was introduce what's called a

“champion/challenger” model setup. Here’s how it works: the bank runs multiple AI models at the same time, like a competition. Each model tries to detect fraud, and the one that does the best job — meaning it’s accurate and fast — becomes the “champion.” That model is then used in their live system. Meanwhile, new challenger models keep being tested in the background. If one of them starts performing better than the current champion, it takes over. This way, the bank's system keeps improving over time and stays ahead of new fraud tricks — all without needing to shut down or rebuild the system from scratch.

The implementation of AI-driven fraud detection at Danske Bank resulted in the following outcomes: a 60% reduction in false positives, with expectations of achieving up to 80%. And a 50% increase in accurate fraud detection rates. Significant time and cost savings by reducing the manual investigation of non-fraudulent transactions. Improved customer experience due to fewer incorrect transaction blocks. By incorporating details like transaction time, location, and user history, the AI system allowed investigators to zero in on truly suspicious activities, helping to simplify and speed up the fraud detection process.

The transition to AI-powered fraud detection involved several technical and organizational hurdles, system limitations, required infrastructure upgrades, and integration with modern cloud and data platforms. Data quality issues and fragmentation caused challenges in training effective machine learning models. Human analysts were still needed for complex edge cases and system supervision. Because fraud tactics are constantly changing, the AI models had to be regularly retrained to stay accurate. To manage this, Danske Bank brought together fraud investigators, data engineers, and compliance experts to work closely as a team, making sure the system stayed effective, secure, and in line with all regulations.

Danske Bank effective and successful use of Deep learning for fraud detection shows how AI can revolutionize the way financial institutions handle security. It proves that AI can go beyond the limits of traditional systems by accurately identifying fraud, reducing unnecessary alerts, and offering a solution that can grow and adapt over time. For financial institutions seeking to modernize their fraud prevention strategies, this case underscores the importance of investing in high-quality data, adaptive model architectures, and interdepartmental collaboration.

References

Danske Bank fights fraud with deep learning and ai. (n.d.-a). https://assets.teradata.com/resourceCenter/downloads/CaseStudies/CaseStudy_EB9821_Danske_Bank_Saves_Millions_Fighting_Fraud_With_Deep_Learning_and_AI.pdf

Donahue, J. (2022, March 3). *Danske Bank and Teradata implement AI to monitor fraud*. Danske Bank and Teradata Implement AI to Monitor Fraud. https://www.teradata.com/press-releases/2017/danske-bank-and-teradata-implement-ai

Fraud-X: An Integrated AI, Blockchain, and Cybersecurity Framework with Early Warning Systems for Mitigating Online Financial Fraud: A Case Study from North Macedonia | IEEE Journals & Magazine | IEEE Xplore, ieeexplore.ieee.org/document/10908824. Accessed 30 June 2025.

Flinders, Mesh, et al. "AI Fraud Detection in Banking." *IBM*, 30 Apr. 2025, www.ibm.com/think/topics/ai-fraud-detection-in-banking.

KSS. (2023). A Survey of Machine Learning Techniques in Financial Fraud Detection. Knowledge Smart Society.

Marla, Deekshith. "The Role of AI and Machine Learning in Fraud Detection." *Arya.Ai: Enterprise-Grade AI Solutions*, Lithasa Technologies Pvt. Ltd., 11 June 2025, arya.ai/blog/ai-and-machine-learning-in-fraud-detection.

Think Big Analytics. (2017). Danske Bank Fights Fraud With Deep Learning and AI. Retrieved from http://www.thinkbiganalytics.com