Alhassane Samassekou

ITAI 2372

# A04 AI in Fraud Detection Case Study

## A case study of Danske Bank

Danske Bank, one of the largest financial institutions in Northern Europe, serves over 3.3 million retail customers and offers a wide range of banking services, including personal banking, corporate banking, and wealth management. With the rise of digital banking, the bank faced increasing challenges in detecting and preventing fraudulent activities, such as payment fraud, identity theft, and account takeovers. Traditional rule-based systems were no longer sufficient to handle the sophistication and volume of modern fraud schemes. To address this, Danske Bank turned to artificial intelligence (AI) to enhance its fraud detection capabilities.

## Technology Overview

Danske Bank uses machine learning for fraud detection. Key technologies include:

- **Machine Learning Models**: Supervised learning uses labeled data to detect fraud, while unsupervised learning identifies unusual patterns.
- **Real-Time Monitoring**: The system processes millions of transactions daily, flagging suspicious activities instantly.
- **Anomaly Detection**: AI analyzes transaction amounts, locations, and user behavior to spot fraud.

- **Natural Language Processing (NLP)**: NLP detects phishing attempts in customer communications.
- **Cloud Infrastructure**: The bank uses cloud computing to handle large data volumes and ensure scalability.

The AI system learns from new data, improving its accuracy over time. For example, it flags unusual activities, like large transactions in foreign countries, for review.

**Benefits**

AI has brought significant benefits to Danske Bank:

- **Higher Detection Rates**: Fraud detection improved by 50%.
- **Fewer False Alarms**: False positives dropped by 60%, reducing disruptions for customers.
- **Cost Savings**: The bank saved millions by preventing fraud and automating manual reviews.
- **Customer Trust**: Faster and more accurate fraud detection boosted customer satisfaction.
- **Scalability**: The system handles growing transaction volumes as the bank expands.

For instance, the AI system once stopped a phishing scam, preventing a €500,000 loss.

**Challenges**

Implementing AI wasn’t without challenges:

- **Data Quality**: Ensuring clean and consistent data was critical for accurate predictions.
- **Model Transparency**: AI’s "black box" nature made it hard to explain decisions, raising concerns for regulators and customers.
- **Ethical Issues**: Handling sensitive customer data required compliance with GDPR.
- **Employee Resistance**: Some staff feared job loss or lacked understanding of AI, which the bank addressed through training.
- **High Costs**: Developing and deploying AI required significant investment.

Danske Bank overcame these by partnering with AI vendors, training employees, and establishing strong governance frameworks.

**Cyberattack and Adaptation**

In 2021, Danske Bank faced a major cyberattack involving phishing and social engineering. Attackers tricked customers into revealing login details, leading to unauthorized transactions.

**How They Were Attacked**

- **Phishing Emails**: Fraudsters sent fake emails mimicking the bank’s official communications.
- **Account Takeovers**: Stolen credentials were used to access customer accounts.

- **Social Engineering**: Attackers created urgency, like claiming accounts were compromised.

**How They Adapted**

Danske Bank responded effectively:

- **Enhanced AI Monitoring**: The system was updated to detect unusual login patterns and transactions.
- **Multi-Factor Authentication (MFA)**: Added security steps for high-risk transactions.
- **Customer Education**: Launched campaigns to teach customers about phishing scams.
- **Collaboration with Authorities**: Worked with law enforcement to track attackers.

The AI system played a key role in blocking fraudulent transactions during the attack.

**Conclusion**

Danske Bank's use of AI for fraud detection has transformed its ability to combat fraud, saving costs and improving customer trust. However, challenges like data quality, transparency, and employee resistance had to be addressed.

The 2021 cyberattack showed the importance of adapting to new threats. Danske Bank's quick response, including AI updates, customer education, and collaboration with authorities, demonstrated its commitment to security.

For other banks considering AI, the key lessons are:

- Invest in quality data and robust AI models.
- Address ethical and regulatory concerns.
- Train employees and foster collaboration.
- Continuously adapt to evolving threats.

AI will remain vital in staying ahead of fraud in the financial sector.

**References**


- AI.Business. (n.d.). *Danske Bank uses AI to enhance fraud detection*. Retrieved from https://www.ai.business
- DigitalDefynd. (n.d.). *AI applications in finance: Case studies*. Retrieved from https://www.digitaldefynd.com
- KnE Social Sciences. (2022). *AI in financial fraud detection*. Retrieved from https://www.knesocialsciences.com
- Cybersecurity Report: Danske Bank Phishing Attack (2021). Retrieved from https://www.cybersecuritynews.com

## 6 other Case Studies of AI in Fraud Detection

### 1. PayPal

**Introduction** PayPal, a global digital payments leader, processes millions of transactions daily, making AI-driven fraud prevention essential.

**Technology Overview** PayPal employs machine learning for real-time fraud detection using:

- **Neural Networks** for anomaly detection.
- **Ensemble Learning** to improve accuracy.
- **Real-time Monitoring** to assess risks.

**Notable Attacks and Adaptation**

- **Credential Stuffing (2010)**: AI-driven behavioral analysis helped detect unauthorized logins.
- **Phishing Attacks (2013)**: NLP enhancements blocked fraud attempts.
- **Botnet Fraud (2021)**: AI-based monitoring mitigated automated threats.

**Benefits & Challenges** AI has reduced fraud, improved user experience, and scaled detection. Challenges include evolving fraud tactics, data privacy concerns, and regulatory compliance.

## 2. JPMorgan Chase

**Introduction** JPMorgan Chase, one of the largest U.S. banks, uses AI to enhance security and prevent fraud across its digital banking services.

**Technology Overview**

- **Deep Learning** to analyze vast transaction datasets.
- **AI-powered Risk Models** for real-time fraud detection.
- **Behavioral Biometrics** to identify fraudulent activities.

**Notable Attacks and Adaptation**

- **Synthetic Identity Fraud**: AI models detect fabricated identities in loan applications.
- **Wire Transfer Fraud Attempts**: Real-time AI detection prevented unauthorized transactions.

**Benefits & Challenges** AI-driven fraud prevention has minimized financial losses. Challenges include balancing security with customer experience and regulatory compliance.

## 3. HSBC

**Introduction** HSBC, a global financial institution, uses AI to combat money laundering and fraud.

**Technology Overview**

- **AI-driven Transaction Monitoring** to detect unusual patterns.

- **Natural Language Processing (NLP)** for analyzing unstructured data.

**Notable Attacks and Adaptation**

- **Money Laundering Cases**: AI-enhanced fraud detection helped HSBC comply with AML regulations.
- **Account Takeover Attacks**: Behavioral analytics minimized unauthorized access.

**Benefits & Challenges** Improved fraud detection and compliance, but challenges exist in data privacy regulations and false positives.

**4. Mastercard**

**Introduction** Mastercard leverages AI to enhance payment security and detect fraudulent transactions.

**Technology Overview**

- **Decision Intelligence AI** for real-time fraud scoring.
- **Pattern Recognition Algorithms** to detect suspicious activities.

**Notable Attacks and Adaptation**

- **Card Skimming Fraud**: AI-driven transaction analysis reduced fraud losses.
- **E-commerce Fraud**: Adaptive AI models minimized online transaction fraud.

**Benefits & Challenges** AI has increased transaction security and reduced fraud losses, but high computational costs remain a challenge.

**5. Citibank**

**Introduction** Citibank integrates AI to enhance fraud detection and regulatory compliance.

**Technology Overview**

- **Machine Learning Algorithms** for analyzing transaction anomalies.
- **AI-driven Risk Assessment** to flag high-risk transactions.

**Notable Attacks and Adaptation**

- **Phishing Scams**: AI-enhanced detection reduced email-based fraud cases.
- **Insider Threats**: Behavioral AI identified suspicious employee activities.

**Benefits & Challenges** Citibank has strengthened fraud prevention, but challenges remain in AI model transparency and adaptability.

**6. Wells Fargo**

**Introduction** Wells Fargo employs AI to secure digital banking and prevent fraud.

**Technology Overview**

- **Real-time AI Fraud Detection** to prevent unauthorized transactions.

- **Biometric Authentication** for enhanced security.

**Notable Attacks and Adaptation**

- **Credential Theft Attacks**: AI-driven anomaly detection helped block unauthorized access.
- **Check Fraud Schemes**: AI improved fraudulent check identification.

**Benefits & Challenges** AI has enhanced fraud detection efficiency, but regulatory challenges and data security concerns persist.

**Conclusion**

AI plays a crucial role in fraud detection across financial institutions. While it enhances security and efficiency, institutions must continuously refine AI models to stay ahead of evolving fraud tactics.