International Journal of Multidisciplinary Research and Growth Evaluation.

Proactive fraud detection: Safeguarding customers with agentic AI

Karan Khanna
Program Manager, USA

* Corresponding Author: **Karan Khanna**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 06
November-December 2024
Received: 10-10-2024
Accepted: 16-11-2024
Page No: 1523-1531

Abstract
Agentic AI is rapidly emerging as a transformative force in the banking industry, poised to revolutionize how customers manage their finances. Unlike traditional AI applications that focus on automating specific tasks, agentic AI systems act as autonomous agents, capable of understanding customer needs, making informed decisions, and taking proactive actions to optimize their financial well-being. This article explores the potential of agentic AI in personalized financial management, examining its key benefits, use cases, and the challenges that lie ahead.

DOI: https://doi.org/10.54660/.IJMRGE.2024.5.6-1523-1531

Keywords: Agentic AI, Banking, Financial assistants, Personalized financial management, Automated savings

Introduction

Understanding the basics of agentic AI in Banking

Agentic AI represents a significant leap forward in artificial intelligence, moving beyond rule-based systems and reactive algorithms. These AI agents can learn from data, adapt to changing circumstances, and interact with customers in a more personalized and human-like manner. In the context of banking, agentic AI can be deployed to create a new generation of intelligent financial assistants that empower customers to achieve their financial goals [1].

Agentic AI systems collect and analyze vast amounts of data from various sources, including customer transactions, market trends, and financial news. This allows them to develop a deep understanding of individual customer needs and preferences. By combining this knowledge with advanced reasoning capabilities, agentic AI can provide tailored financial advice, automate routine tasks, and proactively identify opportunities to improve customers' financial health [2].

Use Cases of Agentic AI in Personalized Financial Management

The applications of agentic AI in personalized financial management are diverse and far-reaching. Some of the key use cases include:

- **Personalized Financial Advice:** Agentic AI can act as a virtual financial advisor, providing customers with personalized recommendations on savings, investments, and debt management. By analyzing spending patterns, risk tolerance, and financial goals, these AI agents can suggest optimal strategies for maximizing returns and achieving long-term financial security [3].
- **Automated Savings and Investment Tools:** Agentic AI can automate the process of saving and investing, making it easier for customers to build wealth over time. These AI agents can analyze income and expenses, identify potential savings opportunities, and automatically allocate funds to investment portfolios based on individual risk profiles and financial goals.
- **Proactive Fraud Detection:** Agentic AI can play a crucial role in protecting customers from financial fraud. By monitoring transactions in real-time and analyzing historical data, these AI agents can identify suspicious activities and alert customers to potential threats. This proactive approach to fraud prevention can help safeguard customer assets and maintain trust in the banking system.
- **Subscription Management:** Agentic AI can help customers manage their subscriptions by analyzing spending patterns,

identifying unused or redundant subscriptions, and suggesting alternatives or cancellations. This can lead to significant cost savings and improved financial health for customers [4].

- Reward Optimization: Agentic AI can help customers maximize reward points earned on their credit cards by analyzing spending habits, recommending optimal card usage strategies, and automatically redeeming rewards for the best value [5].

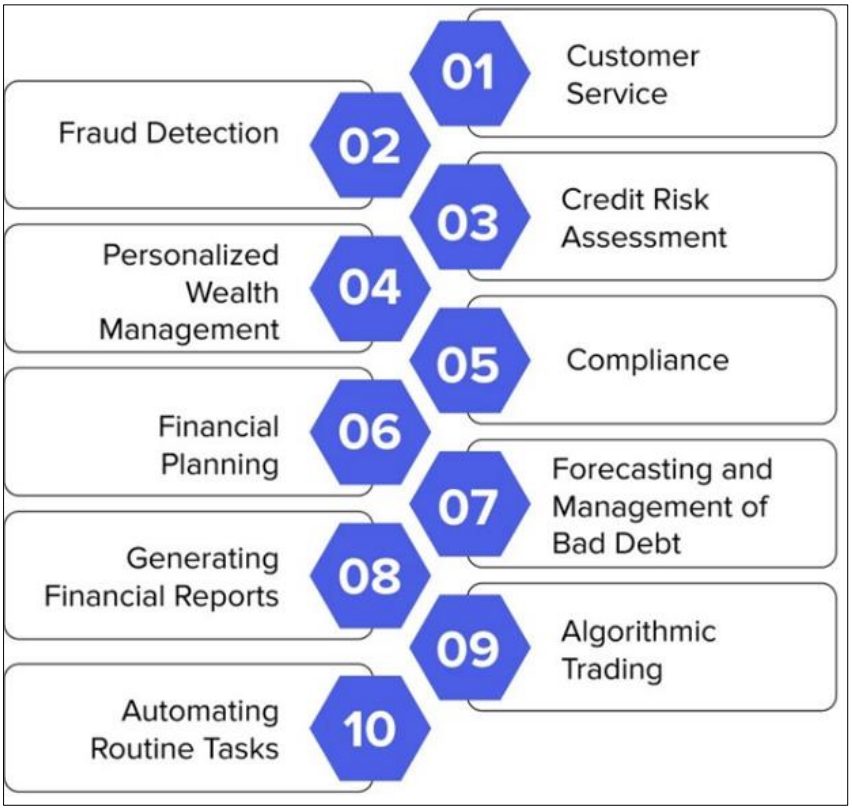

Fig 1: Different use cases of AI in Financial Management

Introduction to Fraud Detection Using Agentic AI

Financial fraud is a pervasive threat to individuals and businesses worldwide, causing significant financial losses and eroding trust in the global economy. Traditional fraud detection methods, often reactive in nature, investigate incidents after they occur, leading to substantial damage. To combat this growing problem, a paradigm shift towards proactive fraud detection is essential.

Proactive fraud detection, powered by Agentic AI, offers a transformative solution by identifying and mitigating potential threats in real-time. This approach leverages cutting-edge technologies to analyze real-time data, historical trends, and behavioral patterns to predict and prevent future fraudulent activities[6]. The increasing complexity of financial systems and the rising sophistication of fraudsters necessitate advanced solutions like AI to safeguard these systems [6].

Notably, financial institutions, including banks, faced nearly $5 billion in fines in 2022 for breaches related to Anti-Money Laundering (AML), sanctions, and Know Your Customer (KYC) regulations, highlighting the urgent need for robust fraud prevention measures [7]. This paper delves into the concept of proactive fraud detection, explores the role of AI in its implementation, discusses the benefits and challenges associated with it, provides real-world examples of successful implementations, and addresses the ethical considerations surrounding its use.

Proactive Fraud Detection: A Paradigm Shift

Proactive fraud detection represents a fundamental shift from reactive approaches to fraud prevention. Instead of merely investigating past incidents, proactive measures focus on predicting and preventing future fraudulent activities. This forward-looking approach is critical in safeguarding customer assets and maintaining the integrity of the financial system. While traditional methods often rely on analyzing historical data to identify patterns of fraud, proactive fraud detection utilizes advanced technologies like AI to analyze real-time data streams, historical trends, and behavioral patterns to identify potential threats before they materialize.

This shift from reaction to preemption is crucial in today's dynamic financial landscape, where fraudsters constantly adapt their tactic [6].

The Role of AI in Proactive Fraud Detection

Agentic AI plays a central role in proactive fraud detection by enabling the analysis of massive datasets with unparalleled speed and accuracy. These AI agents can perform various functions to prevent fraud:

- **Monitor Transactions in Real-time:** AI algorithms can analyze millions of transactions per second, identifying suspicious activities based on predefined rules or deviations from established patterns. For instance, a bank can implement a real-time transaction analysis

solution with AI to analyze 500 transactions per second, enabling immediate detection and prevention of fraud [8].

- **Analyze Historical Data:** AI systems can learn from past fraud patterns, identifying trends and anomalies that may indicate future fraudulent activities. This ability to learn from historical data and continuously improve detection capabilities is a key advantage of AI in fraud prevention [6].
- **Identify Suspicious Activities:** By combining real-time monitoring with historical data analysis, AI agents can flag potentially fraudulent transactions, account takeovers, or identity theft attempts. For example, if a sudden surge in transactions originates from a single account or an unexpected login occurs from a different location, the AI system can generate alerts [9].
- **Alert Customers to Potential Threats:** AI can provide timely alerts to customers about suspicious activities, enabling them to take immediate action to protect their accounts.
- **Predict New Fraud Trends:** AI can analyze large datasets to identify emerging fraud patterns, helping organizations stay ahead of potential threats. This predictive capability allows organizations to proactively implement security measures to counter new fraud tactics [9].

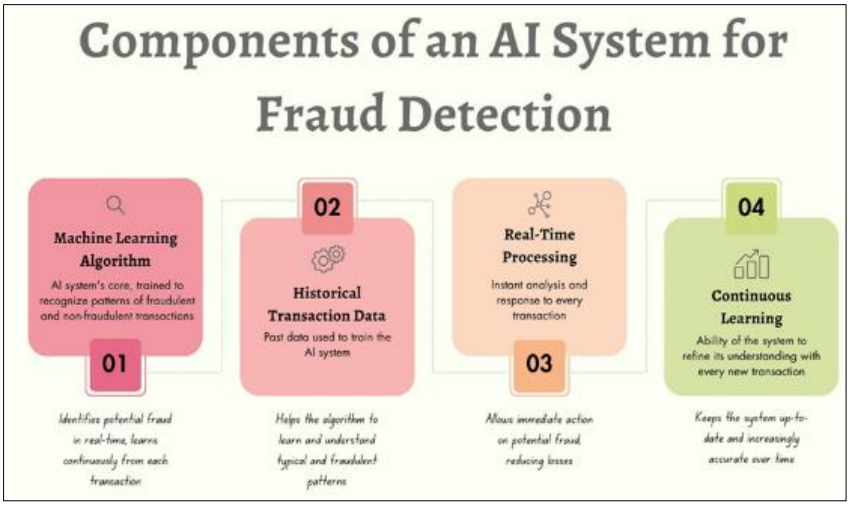

Fig 2: Main Components of an AI system for Fraud Detection

In addition to these core functions, AI utilizes various techniques to enhance fraud detection

- **Machine Learning (ML):** Supervised learning models, such as decision trees and neural networks, are extensively used to identify fraudulent transactions by learning from historical data. These models can distinguish between legitimate and fraudulent transactions by recognizing subtle patterns that might be missed by traditional rule-based systems [10].
- **Deep Learning:** Deep learning models, a subset of ML, can analyze complex patterns and uncover hidden relationships in data, further improving fraud detection accuracy.
- **Natural Language Processing (NLP):** NLP aids in detecting fraudulent activities by analyzing textual data, such as emails and transaction descriptions, to identify suspicious language and patterns [10].

Graph Neural Networks (GNNs): GNNs are employed for their ability to reveal suspicious activity by mapping out the relationship between different pieces of information to better understand the overall context. They can analyze billions of records and identify previously unknown patterns of activity, such as an account sending a transaction to a suspiciousaccount[7].

- **Captcha/reCaptcha:** Captcha and reCaptcha are automated tests used to differentiate between humans and computers, preventing automated fraud attempts such as account creation by bots [11].

Furthermore, specific AI algorithms are employed for fraud detection:

Algorithm	Description	Application in Fraud Detection
Logistic Regression	A statistical model used to predict binary outcomes (e.g., fraud/no fraud) based on a set of independent variables.	Predicting the probability of a transaction being fraudulent.
Decision Trees	A tree-like model that makes predictions based on a series of decision rules inferred from the data.	Classifying transactions as fraudulent or legitimate based on various features.
Random Forests	An ensemble learning method that combines multiple decision trees to improve accuracy and robustness.	Enhancing the accuracy of fraud detection by combining the predictions of multiple decision trees.
XGBoost	A gradient boosting algorithm known for its high accuracy and efficiency.	Improving fraud detection performance by iteratively refining the model to minimize errors.
Neural Networks	Complex models inspired by the human brain, capable of learning intricate patterns in data.	Detecting complex fraud patterns and anomalies that may be missed by simpler algorithms.
Autoencoders	Neural networks used for anomaly detection by learning the normal patterns in data and flagging deviations.	Identifying unusual transactions that deviate from typical customer behavior.

Fig 3: Different types of AI Algorithms and their applications in Fraud Detection

Benefits of AI-driven Proactive Fraud Detection

The integration of AI in proactive fraud detection offers numerous advantages:

- **Enhanced Accuracy:** AI algorithms can analyze vast amounts of data with greater accuracy than traditional methods, reducing false positives and improving fraud detection rates. This leads to more efficient fraud prevention and minimizes the disruption of legitimate transactions [14].
- **Real-time Detection:** AI enables real-time monitoring of transactions, allowing for immediate detection and prevention of fraudulent activities. This real-time capability is crucial in mitigating losses and preventing further damage [14].
- **Adaptability to Emerging Threats:** AI systems can continuously learn and adapt to new fraud tactics, ensuring ongoing protection against evolving threats. This adaptability is essential in the face of constantly changing fraud techniques [14].
- **Cost Savings:** By preventing fraud, AI can help organizations reduce financial losses and operational costs associated with fraud investigation and recovery. This cost-effectiveness makes AI a valuable investment for businesses [14].

Improved Customer Trust: Proactive fraud prevention measures enhance customer trust and confidence in the security of their financial accounts. This increased trust can lead to greater customer loyalty and satisfaction [14].

Challenges and Limitations of AI in Fraud Detection

While AI offers significant benefits for fraud detection, it is essential to acknowledge the challenges and limitations associated with its implementation:

Data Quality and Availability

AI algorithms require access to large volumes of high-quality data for training and accurate predictions. Incomplete, outdated, or inaccurate data can hinder the performance of AI systems. Ensuring data quality and availability is crucial for effective AI-driven fraud detection [15].

False Positives

AI systems can generate false positives, flagging legitimate transactions as fraudulent. This can lead to customer frustration and damage the customer-business relationship. Striking a balance between sensitivity to fraud and minimizing false positives is an ongoing challenge [15].

Bias in Algorithms

AI algorithms can inherit biases present in the training data, potentially leading to unfair or discriminatory outcomes. It is crucial to address potential biases in algorithms and ensure fairness in fraud detection processes [16].

Black Box Operation

The decision-making processes of some AI algorithms can be opaque and difficult to interpret, making it challenging to understand why a transaction was flagged as fraudulent. This lack of transparency can raise concerns about accountability and fairness [16].

Keeping Pace with Evolving Fraud Tactics

Fraudsters constantly develop new tactics, making it challenging for AI systems to keep up with the latest threats. Continuous refinement and updating of AI models are necessary to maintain effectiveness against evolving fraud techniques [17].

Human Oversight

While AI is a powerful tool for fraud detection, it is important to recognize that human judgment is still crucial. AI systems may not always be able to interpret complex scenarios or understand the nuances of human behavior. Human oversight is necessary to ensure accurate interpretation of AI results and handle situations that require human intervention [17].

Successful Implementations of AI-based Fraud Detection Systems

Several organizations across various industries have successfully implemented AI-based fraud detection systems:

- **Financial Institutions:** Major credit card companies like Visa and Mastercard utilize AI to monitor transactions in real-time, significantly reducing fraud rates and enhancing security for cardholders. Visa, for example, employs advanced analytics to detect and flag suspicious transactions, resulting in a notable decrease in fraud rates [18].
- **Insurance Companies:** AI helps insurance companies identify fraudulent claims and potential vulnerabilities in their systems. By analyzing data from past claims, AI can identify areas where fraud is most likely to occur and implement measures to prevent it [19]. For example, Highmark Inc. has generated millions of dollars in savings related to fraud, waste, and abuse, saving approximately $250 million in 2019 and over $850 million in the last five years using fraud detection AI [20].
- **Ride-hailing Industry:** AI is used to identify fake drivers and riders by analyzing location, booking patterns, and payment methods. This helps prevent incidents like fake rides, ghost drivers, or fake reviews, improving safety and security for both drivers and passengers [19].
- **Technology Companies:** Google employs AI to block over 99.9% of phishing attempts targeting Gmail users. This high success rate is attributed to the system's ability to analyze email content, sender reputation, and user behavior patterns to detect and prevent phishing attempts [18].
- **Banking:** JP Morgan Chase developed an advanced AI model to enhance its fraud detection capabilities. This model utilizes machine learning algorithms to analyze vast amounts of transaction data in real-time, identifying patterns and anomalies that may indicate fraudulent activity. The AI model continuously monitors transactions, using historical data to build profiles of typical customer behavior. When a transaction deviates significantly from the established pattern, the system flags it for further investigation [21].

Ethical Considerations

The use of AI in fraud detection raises important ethical considerations that must be addressed to ensure responsible and ethical implementation:

- **Privacy:** AI systems must be designed and implemented in a way that respects customer privacy and data protection regulations. Organizations need to ensure that they comply with relevant regulations, such as the

General Data Protection Regulation (GDPR), and safeguard customer data [15[.

- **Bias and Discrimination:** Organizations must ensure that AI algorithms are free from bias and do not discriminate against certain customer segments. This requires careful consideration of the training data and ongoing monitoring of the AI system's outcomes to identify and mitigate potential biases [22].

Transparency and Explain ability: AI systems should be transparent and provide explanations for their decisions, especially when flagging a transaction as fraudulent. This transparency is essential for building trust with customers and ensuring accountability [23].

- **Accountability:** Clear lines of accountability should be established for AI-driven decisions to ensure responsible use and address potential harms. This includes establishing procedures for human review and intervention when necessary [23].
- **Proportionality and Do No Harm:** The use of AI systems in fraud detection must be proportionate to the risks involved and should not go beyond what is necessary to achieve legitimate aims. Risk assessment should be used to prevent potential harms that may result from AI use [24].

The Future of AI in Fraud Detection

The future of AI in fraud detection is promising, with continuous advancements and innovations driving its evolution. As AI technologies mature, we can anticipate several key developments:

- **Improved Accuracy and Efficiency:** AI algorithms will become more sophisticated, leading to even higher accuracy and efficiency in fraud detection. This will result in fewer false positives and more effective prevention of fraudulent activities.
- **Enhanced Personalization:** AI will enable more personalized fraud prevention measures, tailored to individual customer behavior and risk profiles. This personalized approach will improve the customer experience and reduce unnecessary security checks for low-risk individuals.
- **Increased Collaboration:** Increased collaboration between financial institutions and technology companies will foster the development of more robust and comprehensive. AI-based fraud detection solutions. This collaboration will facilitate the sharing of data and expertise, leading to more effective fraud prevention strategies.
- **Emerging Technologies:** New AI technologies, such as federated learning and explainable AI (XAI), will further enhance fraud detection capabilities. Federated learning allows AI models to be trained on decentralized datasets without compromising data privacy, while XAI aims to make AI decision-making more transparent and understandable.
- **Market Growth:** The fraud detection market is expected to experience significant growth, reaching an estimated value of $106 billion by 2027. This growth highlights the increasing importance of AI in fraud prevention and the growing investment in this domain [25].

AI-powered Fraud Detection in Banks

Banks are increasingly utilizing AI to detect and flag suspicious transactions. AI algorithms analyze vast volumes of transactional data in real-time, identifying patterns and anomalies that may indicate fraudulent activity. This includes:

- **Monitoring for unusual activity:** AI systems can detect anomalies in spending patterns, flagging transactions that deviate significantly from a customer's usual behavior [32].
- **Biometric authentication:** Banks use AI-powered biometric authentication, such as facial recognition and fingerprint scans, to verify customer identities and authorize high-value transactions, reducing the risk of unauthorized access [33].
- **Real-time data analysis:** AI systems can instantly check the authenticity of extracted data by comparing it with available datasets and transaction history, speeding up fraud detection and prevention [33].

Generative AI in Fraud Prevention

Generative AI is playing an increasingly important role in fraud prevention. This technology can learn from existing data to generate new content, such as synthetic fraud data, which can be used to train fraud detection models and improve their accuracy [26]. Financial institutions are using generative AI in various ways:

- **Creating synthetic data:** Visa, for example, uses generative AI to create synthetic data that mimics fraudulent payments, helping to train their deep authorization model and improve its ability to score transactions based on risk [26].
- **Predicting compromised cards:** Mastercard employs generative AI to predict the full 16-digit card numbers of compromised cards, enabling banks to block these cards before they can be used for fraudulent transactions [27].

Identifying fraud patterns: Jumio's 360° Fraud Analytics technology uses generative AI to identify complex fraud patterns and fraud rings by analyzing billions of data points across its network [34].

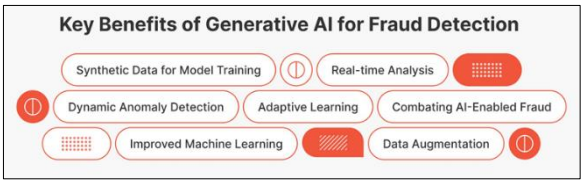

Fig 4: Different use cases for Generative AI

How Financial Institutions are Implementing Agentic AI

Visa

Visa is a leader in implementing Agentic AI to combat fraud. Their Visa Account Attack Intelligence (VAAI) Score tool utilizes generative AI to identify and score enumeration attacks, where fraudsters test stolen card numbers to identify valid ones. VAAI also helps prevent account takeover attacks [30]. The VAAI Score analyzes transaction patterns in real-time, assigning a risk score to each transaction and helping issuers make informed decisions on whether to approve or decline it. This proactive

approach helps prevent fraud before it occurs and reduces operational losses [26].

Visa also employs AI to protect against account-to-account (A2A) fraud. Their "Visa Protect for A2A Payments" service, launched in the United Kingdom, uses AI to identify fraudulent A2A transactions in real-time. In a pilot program, this service identified an additional 54% of fraud beyond that detected by banks' existing fraud prevention systems [36].

Furthermore, Visa Analytics Platform has helped financial institutions like Coastal Federal Credit Union significantly reduce fraud losses. By using the platform's fraud report benchmarking, Coastal Federal Credit Union reduced their annual international fraud from $244,000 to less than $145,000 over a period of four quarters [37].

Mastercard

Mastercard is leveraging Agentic AI to enhance its fraud detection capabilities. Their Consumer Fraud Risk (CFR) solution analyzes multiple data points associated with a transaction, providing a real-time risk score to the sender's bank. This enables banks to potentially identify and halt fraudulent payments before they are processed [38].

Mastercard has also developed a generative AI-based system that predicts the full 16-digit card numbers of compromised cards. This information allows banks to block suspect cards more rapidly, potentially preventing millions of dollars in fraudulent transactions [27].

Mastercard utilizes behavioral biometrics to enhance fraud detection. Their AI systems monitor unique user behaviors, such as typing speed, swipe patterns, and device usage habits, to establish a baseline of normal activity. Deviations from these patterns during a transaction are flagged as potentially fraudulent [38].

According to industry reports, Mastercard has improved fraud detection and reduced false positives tenfold by using Amazon Web Services (AWS) AI and machine learning (ML) services. This has resulted in billions of dollars in merchant savings and a better experience for customers [39].

Feedzai

Feedzai, a leading provider of financial crime prevention solutions, offers a range of AI-powered tools to combat fraud. Their Digital Trust platform analyzes the dynamic context of each transaction, including device information, network data, and geolocation, to identify and prevent money mule scams. By mapping the interrelationships between users and their environment, Feedzai can identify the origin of attacks and proactively block fraudulent accounts [40].

Feedzai also collaborates with Form3 to provide a solution that detects and prevents authorized push payment (APP) fraud. This solution analyzes both sender and beneficiary behavior in real-time, identifying fraud patterns missed by conventional systems [41].

Recent findings suggest that Feedzai has helped a major UK bank improve its fraud detection rate by 30%, preventing millions in potential scam losses [42]. In another case study, an Australian payments provider using Feedzai's solution cut fraud losses by 114% [43].

Jumio

Jumio specializes in AI-powered identity verification and risk assessment. Their platform employs advanced machine learning algorithms to verify government-issued IDs in real-time, detecting digital manipulations and preventing fraudulent account creation [44].

Jumio's 360° Fraud Analytics technology uses AI-driven predictive analytics to identify fraud patterns with greater sophistication and accuracy. By analyzing billions of data points across its network, Jumio can identify fraud rings and other coordinated attacks, preventing fraud before it occurs [34]. Jumio's solutions have helped companies like Revolut achieve positive results in the form of higher conversions, an enhanced onboarding experience for new customers, and lower fraud rates [20]. Industry reports indicate that Jumio's fraud detection technology has improved fraud detection rates by at least 30% [34].

DataVisor

DataVisor offers an AI-powered fraud and risk platform that combines unsupervised and supervised machine learning to detect and prevent fraud across various industries. Their platform can process massive amounts of data in real-time, enabling rapid response to emerging fraud attacks [46].

DataVisor's solutions have helped financial institutions achieve significant reductions in fraud losses and false positives. For example, a top payment network using DataVisor's platform achieved a 20% uplift in fraud detection with 94% accuracy [47]. In another case study, a top U.S. credit card issuer reduced fraud losses by $15 million using DataVisor's platform [48].

Company	AI Technologies Used	Fraud Reduction Rate
Visa	Generative AI, Deep Learning	Reduced false positives by 85% in enumeration attacks [5]
Mastercard	Generative AI, Graph Technology, Behavioral Biometrics	Doubled the detection rate of compromised cards [24]
Feedzai	Machine Learning, Behavioral Biometrics	Improved fraud detection rate by 30% for a major UK bank [17]
Jumio	Machine Learning, AI-driven predictive analytics	Improved fraud detection rate by at least 30% [9]
DataVisor	Unsupervised and Supervised Machine Learning	20% transaction fraud detection uplift for a top payment network [22]

Specific AI Technologies Used and Fraud Reduction Rates

Cost Savings with Agentic AI

Beyond preventing fraudulent transactions, Agentic AI offers significant cost-saving benefits for financial institutions. By automating tasks, minimizing manual reviews, and preventing fraud losses, Agentic AI can help reduce operational costs. For example, Coastal Federal Credit Union reduced operational costs by minimizing the number of cards that needed to be reissued due to fraud [36]. Similarly, a large North American retail bank saved $30 million over three years by implementing Feedzai's hybrid fraud detection solution [31].

Conclusion

Proactive fraud detection, powered by Agentic AI, represents a paradigm shift in combating financial fraud. By leveraging AI's ability to analyze vast amounts of data, identify suspicious activities, and predict emerging threats, organizations can effectively protect their customers and maintain trust in the financial system. While challenges and ethical considerations remain, the continuous advancement of AI technologies promises a future where financial fraud is minimized, customer trust is strengthened, and the integrity of the financial system is preserved.

However, it is crucial to acknowledge the potential drawbacks of AI in fraud detection, such as the risk of bias, the need for high-quality data, and the importance of human oversight. Striking a balance between leveraging the power of AI and addressing its limitations is essential for responsible and effective fraud prevention. As AI technologies continue to evolve, ongoing research and development will be crucial to ensure that AI-based fraud detection systems remain effective, ethical, and adaptable to the ever-changing landscape of financial crime.

References

1. Bank of America Institute. The new wave: Agentic AI. Accessed September 10, 2024. Available from: https://institute.bankofamerica.com/transformation/agentic-ai.html
2. Akira AI. Revolutionizing Banking Operations with Agentic AI. Accessed September 10, 2024. Available from: https://www.akira.ai/blog/banking-operations-with-ai-agents
3. Bud Financial. Agentic banking platform. Accessed September 10, 2024. Available from: https://www.thisisbud.com/en-us/agentic
4. Compare the Cloud. The Role of Artificial Intelligence in Subscription Management. Accessed September 10, 2024. Available from: https://www.comparethecloud.net/articles/the-role-of-artificial-intelligence-in-subscription-management/
5. Xoxoday. What are AI Rewards & How Does it Personalize Recognition. Accessed September 10, 2024. Available from: https://www.xoxoday.com/glossary/ai-rewards
6. International Journal of Science and Research Archive. Artificial Intelligence in fraud detection: Revolutionizing financial security. Accessed September 10, 2024. Available from: https://ijsra.net/sites/default/files/IJSRA-2024-1860.pdf
7. NVIDIA Blog. How Is AI Used in Fraud Detection? Accessed September 11, 2024. Available from: https://blogs.nvidia.com/blog/ai-fraud-detection-rapids-triton-tensorrt-nemo/
8. Evertec Inc. The role of artificial intelligence (AI) in fraud detection: key statistics and applications. Accessed September 11, 2024. Available from: https://www.evertecinc.com/en/the-role-of-artificial-intelligence-ai-in-fraud-detection-key-statistics-and-applications/
9. Fingerprint. The latest trend in fighting fraud: AI for fraud detection. Accessed September 11, 2024. Available from: https://fingerprint.com/blog/ai-fraud-detection/
10. ResearchGate. Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Accessed September 12, 2024. Available from: https://www.researchgate.net/publication/383264952_Artificial_intelligence_in_fraud_prevention_Exploring_techniques_and_applications_challenges_and_opportunities
11. Trustpair. AI for fraud detection: the complete guide. Accessed September 12, 2024. Available from: https://trustpair.com/blog/ai-for-fraud-detection-the-complete-guide/
12. TrustDecision. 5 New Fraud Detection Machine Learning Algorithms. Accessed September 12, 2024. Available from: https://trustdecision.com/resources/blog/5-new-machine-learning-algorithms-for-fraud-detection
13. SQream. Best Machine Learning Algorithms for Fraud Detection. Accessed September 12, 2024. Available from: https://sqream.com/blog/fraud-detection-machine-learning/
14. SmartDev. AI in Financial Fraud Detection: The Comprehensive Guide 2025. Accessed September 13, 2024. Available from: https://smartdev.com/ai-driven-fraud-detection/
15. DigitalOcean. Understanding AI Fraud Detection and Prevention Strategies. Accessed September 15, 2024. Available from: https://www.digitalocean.com/resources/articles/ai-fraud-detection
16. CyberDB. The Advantages and Drawbacks of AI and Machine Learning in Fraud Detection. Accessed September 15, 2024. Available from: https://www.cyberdb.co/the-advantages-and-drawbacks-of-ai-and-machine-learning-in-fraud-detection/
17. Anura.io. The Hidden Pitfalls of AI in Fraud Detection: False Positives. Accessed September 20, 2024. Available from: https://www.anura.io/fraud-tidbits/the-hidden-pitfalls-of-ai-in-fraud-detection-false-positives
18. Planet Compliance. The Impact of AI on Fraud Detection Systems. Accessed September 20, 2024. Available from: https://www.planetcompliance.com/ai-fraud-detection-systems/
19. Dojah. Case Studies: AI in Action Against Fraud. Accessed September 20, 2024. Available from: https://dojah.io/blog/ai-in-action-against-fraud-case-studies
20. Superior Data Science. Case Study on Fraud Detection. Accessed September 20, 2024. Available from: https://superiordatascience.com/case-study-on-fraud-detection/
21. Medium. How AI Transformed Financial Fraud Detection: A Case Study of JP Morgan Chase | by

Jeyadev Needhi. Accessed September 21, 2024. Available from: https://medium.com/@jeyadev_needhi/how-ai-transformed-financial-fraud-detection-a-case-study-of-jp-morgan-chase-f92bbb0707bb
22. Moody's. Ethical considerations of AI-powered customer due diligence. Accessed September 21, 2024. Available from: https://www.moodys.com/web/en/us/kyc/resources/insights/applying-ai-to-3-types-customer-due-diligence.html
23. Ethics Sage. Ethical Risks of AI. Accessed September 21, 2024. Available from: https://www.ethicssage.com/2024/04/ethical-risks-of-ai.html
24. UNESCO. Ethics of Artificial Intelligence. Accessed September 22, 2024. Available from: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics
25. SPD Technology. Credit Card Fraud Detection Case Study. Accessed September 23, 2024. Available from: https://spd.tech/machine-learning/credit-card-fraud-detection-case-study/
26. Tech Brew. Inside Visa's AI strategy, from vintage neural networks to synthetic data. Accessed September 10, 2024. Available from: https://www.emergingtechbrew.com/stories/2024/10/29/visa-ai-strategy-rajat-taneja
27. PYMNTS. Mastercard Doubles Fraud Detection Rate With Generative AI. Accessed September 23, 2024. Available from: https://www.pymnts.com/news/security-and-risk/2024/mastercard-deploys-ai-to-combat-card-fraud/
28. Cloud Kinetics. The AI Edge in Fraud Prevention: How Banks & Financial Services Can Fight Fraud With AI-Driven Analytics. Accessed September 23, 2024. Available from: https://www.cloud-kinetics.com/blog/ai-analytics-for-fraud-prevention-in-banks-financial-services/
29. Jumio. Revolutionizing Fraud Detection With AI & Machine Learning. Accessed September 23, 2024. Available from: https://www.jumio.com/machine-learning-fraud-detection/
30. Visa. Visa Announces Generative AI-Powered Fraud Solution to Combat Account Attacks. Accessed September 24, 2024. Available from: https://investor.visa.com/news/news-details/2024/Visa-Announces-Generative-AI-Powered-Fraud-Solution-to-Combat-Account-Attacks/default.aspx
31. Feedzai. Boosts Legacy Fraud Systems for Digital Banking Era. Accessed September 24, 2024. Available from: https://www.feedzai.com/resource/boost-legacy-bank-fraud-systems-for-digital-banking/
32. Infosys BPM. AI-Powered Financial Fraud Detection in Banking. Accessed September 24, 2024. Available from: https://www.infosysbpm.com/blogs/bpm-analytics/fraud-detection-with-ai-in-banking-sector.html
33. Docsumo. Transforming Bank Fraud Detection with Artificial Intelligence (AI): Benefits and Limitations. Accessed September 25, 2024. Available from: https://www.docsumo.com/blog/ai-based-bank-fraud-detection
34. Jumio. Jumio Disrupts Identity Verification Market with Groundbreaking New Fraud Prevention Technology. Accessed September 25, 2024. Available from: https://www.jumio.com/about/press-releases/new-fraud-prevention-technology/
35. PYMNTS. Visa: AI Helped Block 80 Million Fraudulent Transactions in 2023. Accessed September 25, 2024. Available from: https://www.pymnts.com/artificial-intelligence-2/2024/visa-ai-helped-block-80-million-fraudulent-transactions-in-2023/
36. Visa. Reducing international fraud loss. Accessed September 25, 2024. Available from: https://usa.visa.com/content/dam/VCOM/regional/na/us/partner-with-us/documents/vap-coastal-fcu-case-study.pdf
37. FinTech Magazine. Mastercard Expands AI Tool to Fight Payment Fraud and APP Scams. Accessed September 25, 2024. Available from: https://fintechmagazine.com/articles/mastercard-enhances-ai-tool-to-combat-payment-fraud
38. DigitalDefynd. 5 Ways MasterCard is Using AI [Case Study][2025]. Accessed September 25, 2024. Available from: https://digitaldefynd.com/IQ/ways-mastercard-use-ai/
39. AWS. Mastercard Uses AWS AI and ML Services to Detect and Prevent Fraud. Accessed October 1, 2024. Available from: https://aws.amazon.com/solutions/case-studies/mastercard-ai-ml-testimonial/
40. Feedzai. Feedzai's Digital Trust Helps Challenger Bank Take on Money Mule Networks and Protect Customers. Accessed October 1, 2024. Available from: https://www.feedzai.com/resource/feedzais-digital-trust-helps-challenger-bank-take-on-money-mule-networks-and-protect-customers/
41. Feedzai. Discover How Feedzai and Form3 Improved APP Fraud Detection. Accessed October 1, 2024. Available from: https://www.feedzai.com/resource/discover-how-feedzai-and-form3-improved-app-fraud-detection/
42. Feedzai. Using Fraud Analytics to Stay Ahead of Criminals. Accessed October 1, 2024. Available from: https://www.feedzai.com/blog/using-fraud-analytics-to-stay-ahead-of-criminals/
43. Feedzai. Australian Payments Provider Increases Fraud Detection by 114%. Accessed October 3, 2024. Available from: https://www.feedzai.com/resource/australian-payments-provider-cuts-fraud-losses-by-114/
44. Jumio. Dribe | Jumio Case Study. Accessed October 3, 2024. Available from: https://www.jumio.com/case-study-dribe/
45. Jumio. Revolut | Jumio Case Study. Accessed October 4, 2024. Available from: https://www.jumio.com/case-study-revolut/
46. Microsoft Partner Network. DataVisor Case Study. Accessed October 4, 2024. Available from: https://partner.microsoft.com/case-studies/DataVisor-rewards
47. DataVisor. Stop Transaction Fraud With Machine Learning. Accessed October 7, 2024. Available from: https://www.datavisor.com/industry-solutions/transaction-fraud/
48. DataVisor. Top Financial Institution Fights Fraudulent Transactions in Real Time. Accessed October 7, 2024. Available from:

https://www.datavisor.com/intelligence-center/case-studies/moneytransferfraud/
49. Mastercard. Mastercard Accelerates Card Fraud Detection with Generative-AI Technology. Accessed October 7, 2024. Available from: https://newsroom.mastercard.com/news/press/2024/may/mastercard-accelerates-card-fraud-detection-with-generative-ai-technology/