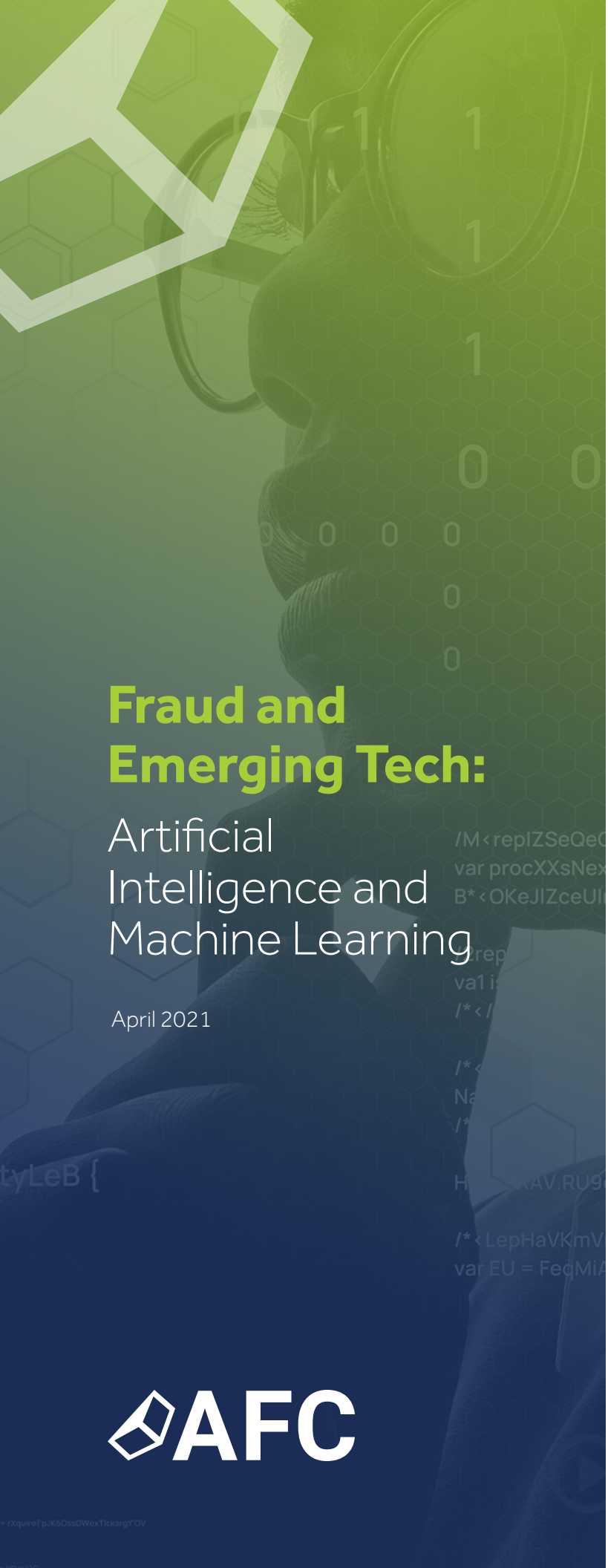

Fraud and Emerging Tech:

Artificial Intelligence and Machine Learning

April 2021

AFC

Artificial intelligence (AI) has become one of the fastest-growing priorities for many companies in the digital era and, consequently, will have a wide-ranging impact on businesses across the globe. This post, part of an emerging technology series from the Anti-Fraud Collaboration, examines the implications of AI and one of its most commonly known applications—machine learning—when it comes to mitigating fraud risk.

WHAT IS AI AND MACHINE LEARNING?

Artificial intelligence (AI) technologies can process unstructured data and automate tasks that previously required human intelligence or judgment, such as extracting meaning from images, text, or speech; detecting patterns and anomalies; and making recommendations, predictions, or decisions.[1] More simply put, AI is any technology that enables a computer to mimic human behaviors and decisions.

AI is an emerging technology that was invented a long time ago—in 1955—yet it can still be difficult to grasp due to its broad and far-reaching nature. That being said, AI technology is pervasive in society and its applications are used by most people daily. Some of the most common everyday examples of AI extend beyond customer service chatbots and self-driving cars. AI is also being used to predict traffic patterns based on smartphone location data for maps (e.g., Google, Waze) and to optimize routes, fares, and surge pricing for rideshare applications (e.g., Uber, Lyft).

1 Deloitte, *Automation with Intelligence: Pursuing Organisation-Wide Reimagination*, 2020.

Numerous applications of AI have enabled companies to create value and experience a wide range of benefits, including improved decision-making, increased efficiency and productivity, cost savings, innovative services and products, and better customer experiences. Consequently, AI is an undeniable trend in digital innovation today. According to PwC's 2021 AI Predictions survey, 86 percent of 1,032 respondents said that AI will be a "mainstream technology" at their company in 2021.

Of the vast capabilities that AI technology can deliver, its portfolio includes machine learning, deep learning, natural language processing, and computer vision. Machine learning is one of the most practical applications of AI; it is used to help companies analyze data, make classifications, automate processes, identify new trends and hidden patterns, and predict future outcomes. Machine learning algorithms can be classified into three pillars:

- **Supervised learning –** Algorithms use existing data to make predictions by training labeled data with feedback from humans to learn the relationship between inputs and a given output.
- **Unsupervised learning –** Algorithms find correlations in data that are improbable for humans to identify by exploring input data without being given an explicit output variable.
- **Reinforcement learning –** Algorithms incorporate rewards and penalties within the model as they learn to perform a task and achieve the desired results by maximizing the rewards they receive for their actions.

Machine learning algorithms have robust capabilities and can be used for a wide range of purposes, including improving automation techniques, increasing efficiency, and identifying anomalies from large datasets. However, using machine learning requires teaming with experts who have a trained dataset and dedicating resources to train the models to become effective.

HOW CAN AI AND MACHINE LEARNING FIGHT FRAUD?

PwC's 2021 AI Predictions survey found that managing risk, fraud, and cybersecurity threats is the most important AI application for companies in 2021. The advancement of AI technology has helped companies conduct more proactive and predictive analytics to detect fraud. Traditional risk-based analyses can evolve and incorporate machine learning algorithms to identify anomalies, which then inform and refine the risk algorithms.

TOP RANKED ARTIFICIAL INTELLIGENCE APPLICATIONS FOR 2021

1. **Managing risk, fraud, and cybersecurity threats**
2. **Improving AI ethics, explainability, and bias detection**
3. **Helping employees make better decisions**
4. Analyzing scenarios using simulation modeling
5. Automating routine tasks

Source: PwC 2021 AI Predictions

Machine learning algorithms can be used to better assess fraud risk factors due to their ability to understand complex relationships among a vast amount of data, including but not limited to, millions of transactions, hundreds of thousands of entity and third-party data, and years of journal entries and company records. As such, the algorithms can produce better outcomes than traditional "rule-based" approaches. Below are examples of how AI and machine learning can be used to fight fraud:

- **Bribery and corruption –** Sales contracts can be reviewed to identify and predict which sales transactions and third parties create the most corruption risk. Higher-risk contracts can be flagged for additional compliance oversight.
- **Disbursements –** Accounts payable data can be analyzed to predict which payments might violate contract terms or present higher risks for inappropriate or fraudulent transactions.

- **Expense fraud –** Expense reports can be interpreted based on a historical set of proven expense fraud cases to identify spending patterns and employee behaviors, and detect suspicious, exaggerated, or falsified expense claims.
- **Third-party risk –** Due diligence data, such as background checks, credit reports, questionnaires, and annual assessments, can be aggregated and reviewed to perform trending analysis and calculate risk scores. Third parties can be compared to one another to identify patterns, relationships, and anomalies.
- **Vendor fraud –** Invoices can be scanned and grouped into categories to identify commonalities or disparities in an effort to identify vendor fraud. Anomalies can be flagged for further review.

Although AI technology assists with identifying fraud risks, one cannot understate the importance of appropriate human intervention. Companies should avoid the risk of over-relying on data and AI-driven decisions alone, as it is important for companies and auditors alike to be able to interpret the data and make important judgments, especially once red flags and warning signs are detected.

Further, AI's data, technology, and talent may be decentralized across different locations, business functions, and multiple third parties, which can pose challenges and risks for companies and their executives. AI is a complex technology that is not yet fully understood. While reaping the benefits of AI, it is also important to balance the risks and rewards.

WHAT ARE RISKS OR OTHER KEY CONSIDERATIONS RELATED TO AI AND MACHINE LEARNING?

One of the biggest challenges with AI and machine learning is that the technology keeps changing and adapting. Companies need to be involved and pay attention to their AI technology and related data from the inception stages of designing the model, through the development, deployment, and iterative adjustment stages. The risks in the table below should be considered when implementing AI technology.

CONCLUSION

AI is a powerful technology that is ever evolving and continually changing as it learns. Therefore, it is incumbent on companies to strive beyond the basics of implementation. Responsible AI use not only ensures that the model is providing value and robust performance, but also establishes trust and protects sensitive data on which critical business decisions are made. For forward-looking companies seeking to embrace AI, accelerating and enhancing governance to keep up with AI is as critical as improving and reinforming the technology.

AI Risks and Considerations

WHAT IS THE RISK?	HOW TO MITIGATE THE RISK?
Control risk – Lack of human agency in AI-supported processes and inability to control rogue AI.	Implement and monitor **robust controls** that cover every stage of the AI life cycle.
Compliance risk – Noncompliance with applicable laws and regulations.	Ensure AI is **up-to-date and compliant** with local privacy laws and industry regulations.
Ethical risk – Lack of values or value misalignment further perpetuate biases.	Establish **trust** in your AI system and address **ethical issues** such as fairness.
Performance risk – Risk of errors, biases, and performance instability.	Monitor, report, and improve **AI model performance** on an ongoing basis.
Security risk – Adversarial attacks, cyber intrusion and privacy risks, and open-source software vulnerabilities.	Establish and improve **defense mechanisms** against cyber threats and intrusions.

Where can I learn more about AI and machine learning?

- BDO: *Getting from A to AI: The Path to Data Analytics Maturity*
- CAQ: *Emerging Technologies: An Oversight Tool for Audit Committees*
- CAQ: *Emerging Technologies, Risk, and the Auditor's Focus*
- Crowe: *AI and Digital Platforms Are Changing the Way We Work*
- Deloitte: *Automation with Intelligence: Pursuing Organisation-Wide Reimagination*
- Deloitte: *Thriving in the Era of Pervasive AI: Deloitte's State of AI in the Enterprise, 3rd Edition*
- EY: *How to Move AI from Magical to Practical*
- FEI: *3 Ways to Improve Financial Management with AI in 2021*
- Grant Thornton: *The Smart Approach to Intelligent Automation*
- The IIA: *Internal Audit's Role in AI Success*
- KPMG: *The Shape of AI Governance to Come*
- NACD: *Technology Brief: A Board Primer on Artificial Intelligence*
- NACD: *The How, Why, and What of Artificial Intelligence*
- PwC: *2021 AI Predictions Survey*
- PwC: *Sizing the Prize: What's the Real Value of AI for Your Business and How Can You Capitalise?*
- RSM: *Artificial Intelligence Is Not Taking Over Your Job—It's Enhancing It*

AFC

www.antifraudcollaboration.org

We welcome your feedback!

Please send your comments or questions to antifraudcollaboration@thecaq.org