CRA Insights

Risk, Investigations & Analytics

CRA Charles River Associates

October 2024

Navigating the intersection of innovation and regulation: Addressing fraud risks in the age of artificial intelligence ("AI")

In recent years, the rise of AI and generative artificial intelligence (GenAI) has been impactful to many industries. From generating realistic text to creating lifelike pictures, images and other content, it has opened up a world of possibilities for users and organizations alike. However, as with any powerful tool, there are inherent risks that organizations must navigate to responsibly harness GenAI's full potential. Recognizing these challenges, regulators like the Department of Justice (DOJ) have introduced measures to promote the responsible and ethical use of the technology.

In February 2024, the Deputy Attorney General, Lisa Monaco, announced that individuals convicted of crimes involving the use of AI may face longer sentences, reflecting the increasing recognition of AI's potential for misuse and its exploitation for fraud and criminal activities. Additionally, the DOJ announced the launch of the initiative *Justice AI,* to ascertain how the Department can "ensure [they] accelerate AI's potential for good while guarding against its risks."[1] These developments underscore the need for organizations to proactively address the risks associated with AI, particularly in light of evolving regulatory regulations and frameworks.

Further, in April 2024, the National Institute of Standards and Technology (NIST), an agency of the US Department of Commerce, announced its Generative Artificial Intelligence Profile.[2] The profile provides guidelines for organizations implementing AI with an emphasis on risk management and compliance.[3] By offering a framework that balances innovation with caution, the profile encourages

---

1 Monaco, Lisa, "Deputy Attorney General Lisa O. Monaco Delivers Remarks at the University of Oxford on the Promise and Peril of AI," Oxford, UK, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and.

2 The profile is a publication based on NIST's AI Risk Management Framework (AI RMF) to help companies identify and manage unique risks posed by GenAI.

3 "AI Risk Management Framework," NIST, https://www.nist.gov/itl/ai-risk-management-framework.

organizations to not only focus on maximizing AI's benefits but also on mitigating associated risks, including data privacy concerns, bias in algorithms, and security vulnerabilities.

More recently, in September 2024, Nicole Argentieri, principal deputy assistant attorney general and head of the DOJ's Criminal Division, stated at a Society of Corporate Compliance and Ethics conference, that prosecutors will examine how companies assess and manage the risks associated with new technologies "…such as artificial intelligence both in their business and in their compliance programs."[4] Prosecutors will also evaluate the technology a company uses for business, whether they have assessed the risks of that technology, and if they have implemented measures to address any associated risks.[5]

As regulatory scrutiny intensifies, organizations should stay ahead of these changes by integrating guidelines into their AI strategies. Proactively adapting to these standards will not only help in maintaining compliance but also in fostering trust and credibility with customers, partners, and regulators. In this dynamic landscape, the ability to effectively navigate these regulatory frameworks will become a critical differentiator in organizations' successful use of the technology.

The dual nature of GenAI

GenAI integrates large language models and sophisticated algorithms to generate new information based on continuous training and user input. While products like ChatGPT have been widely used in the market since 2022, the increased adoption of GenAI by private and public organizations brings both opportunities and heightened fraud risks. Organizations should consider implementing robust risk management strategies to, in part, prevent unauthorized access to sensitive information and help mitigate internal and external fraud risks. Governance initiatives such as encrypting sensitive information, anonymizing data and removing personally identifiable information (PII) from models, and conducting due diligence on third-party vendors are examples of valuable risk management measures.

Fraudsters can exploit, for example, GenAI's ability to mimic human behavior and process large volumes of data, accelerating the speed and sophistication of fraud schemes. GenAI's ability to process massive volumes of data quickly can cause damage before organizations even realize something is wrong. The technology can generate false documents and data that are difficult to distinguish from legitimate ones, posing serious threats to businesses. Recent incidents, such as the use of deepfake technology to impersonate company executives in video calls to request fund transfers, highlight the serious implications of GenAI in fraudulent schemes.[6] As Lisa Monaco

---

4 Argentieri, Nicole M., "Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the society of Corporate Compliance and Ethics 23rd Annual Compliance &Ethics Institute," September 23, 2024, Grapevine, TX, https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-society.

5 Argentieri, Nicole M., "Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the society of Corporate Compliance and Ethics 23rd Annual Compliance &Ethics Institute," September 23, 2024, Grapevine, TX, https://www.justice.gov/opa/speech/principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks-society.

6 Chen, Heather and Kathleen Magramo, "Finance worker pays out $25 million after video call with deepfake 'chief financial officer,'" CNN, February 4, 2024, https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html.

.

stated, “AI can lower the barriers to entry for criminals… [as] it’s changing how crimes are committed and who commits them – creating new opportunities for wanna-be hackers and supercharging the threat posed by the most sophisticated cybercriminals.”[7]

Despite the potential of AI technologies to support fraudulent activities, it can also aide organizations with facilitating corporate compliance. Prior to the adoption of building compliance systems using AI/machine learning technology[8], organizations traditionally relied on rules-based fraud detection platforms to monitor business practices and operations, which are limited by human capabilities and lack the complexity to pinpoint various prohibited schemes and misconduct.

Now, identifying patterns linked to fraudulent activities and other financial crimes through GenAI is more efficient and cost-effective than the older, traditional methods. AI technologies continuously learn and improve from new data, enhancing their ability to detect fraudulent activities and anomalies. Additionally, these technologies can be customized and provide an organization with critical insights that can be transformed into strategic actions. For example, GenAI is particularly valuable for producing synthetic data to train fraud detection models when real-world data is unavailable, thereby increasing the robustness of monitoring systems. GenAI can also simulate and produce diverse fraud scenarios to train and increase the strength of monitoring systems and help mitigate against different forms of schemes.

Moreover, AI technologies can help streamline risk assessments of internal controls and compliance frameworks, identifying threats like malicious codes or gaps in internal controls, that may otherwise go unnoticed. AI technologies can also provide organizations the ability for continuous monitoring of transactions and relationships with third parties, alerting management of anything suspicious or out of the ordinary. Once flagged, additional due diligence procedures on the transactions and parties involved can be used to help confirm whether actual fraud has occurred and subsequently assist the organization with creating a plan to mitigate.

As organizations explore AI tools to enhance operations, and to protect themselves in doing so, they should consider establishing best practices and new internal controls around its utilization. This could include guidelines for data privacy, regular audits of AI/ML algorithms and associated internal controls, and employee training. Before organizations begin to implement AI and machine learning systems for fraud detection and compliance, they should consider conducting thorough risk assessments and tailoring AI solutions to their specific needs. This approach can help align these technologies with the organization’s overall risk management strategy, enhancing both operational efficiency and security.

For more information on this topic or to discuss implementing AI into the risk assessment process, please contact Frank Esposito in our Risk, Investigations & Analytics Practice.

---

7 Monaco, Lisa, “Deputy Attorney General Lisa O. Monaco Delivers Remarks at the University of Oxford on the Promise and Peril of AI,” February 14, 2024, Oxford, UK, https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and.

8 Machine learning (ML) is a branch of artificial intelligence (AI) that focuses on developing algorithms using mathematical and statistical models to perform data analyses.

About CRA's Risk, Investigations & Analytics Practice

The Risk, Investigations & Analytics (RIA) Practice is unique in its approach to executing large, multijurisdictional and multidisciplinary investigative, compliance and disputes assignments for clients. These complex matters often require sophisticated data analytics tools combined with unique investigative capabilities and deep subject matter expertise integrated into a single team for efficient delivery of services. By analyzing data collected from disparate sources and utilizing advanced analytics techniques, we can uncover instances and patterns of fraud and previously unknown issues or other problematic activity.

Contacts

Frank Esposito
Principal
+1-212-294-8839
fesposito@crai.com

Lauren Gordon
Associate Principal
+-1-212-294-8888
lgordon@crai.com