Ballard
Spahr
LLP

THE NEW YORK LAW JOURNAL

Artificial Intelligence: Avoiding Pitfalls on the Path Forward

October 2, 2023

By Celia Cohen and Nathaniel Botwinick

The rise of artificial intelligence (AI), and the buzz surrounding it, has many companies embracing its benefits. But as the use of AI increases, so too do the opportunities for criminal activity. As with most new technologies, AI brings new opportunities for progress—while simultaneously providing criminals with new tools to commit malfeasance.

The growth of cryptocurrency, for example, has brought with it an innovative platform upon which to expand conventional frauds. And now, in addition to concerns about AI-powered cybersecurity breaches and deepfakes (with realistic AI-generated video and audio) for criminal purposes, there is also the potential for using AI to commit traditional financial and white-collar crimes, such as insider trading, market manipulation, fraud, and spoofing.

This article examines what companies should do to address the risks of AI, including implementing specific compliance regimes, training programs, risk disclosures and other measures, to best protect clients and customers—and avoid running afoul of law enforcement and government regulators.

AI-Powered Cybersecurity Breaches

One of the biggest risks for companies using AI is cybersecurity breaches. Cyberattacks have been at the forefront of risk to companies for some time, but AI has brought more sophistication to the attacks. AI could help hackers craft phishing emails that appear identical to legitimate emails. And the rise of AI-powered "deepfakes" could allow hackers to impersonate employees' voices and appearances to carry out security breaches. See, e.g., "Increasing Threat of Deepfake Identities", Department of Homeland Security.

Deepfakes also could be used for attacks on corporations—for example, hackers could impersonate a customer's voice to bypass voice authentication and access the customer's accounts. Or nefarious actors could create a deepfake of the CEO making a company announcement in an attempt to manipulate the stock price. Companies, therefore, must be prepared not only to identify such breaches, but also be able to quickly counter them.

In addition to the risk of data exposure that could harm the company and its customers, companies also face the potential for government and regulatory inquiries. In July 2023, the SEC adopted rules that require registrants to disclose material cybersecurity incidents, and on an annual basis, material information regarding their cybersecurity risk management, strategy, and governance. See "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies", SEC Press Release 2023-139, July 26, 2023. Companies that fail to disclose material incidents and their strategies will run the risk of incurring legal liability.

The early response from companies to the SEC's new rule has been to release a flurry of 8-Ks detailing cyberattacks while the company comes to terms with the extent of the attack. See, e.g., Kim S. Nash, "Clorox Cyberattack Brings Early Test of New SEC Cyber Rules", The Wall Street Journal, Sept. 20, 2023. In addition, public companies continue to risk SEC enforcement actions for failing to maintain adequate disclosure controls and procedures. See, e.g., "In the Matter of First American Financial Corp.", Securities Act Release No. 92176 (July 14, 2021).

Accordingly, given the sophistication of AI, companies need to review and revise their cybersecurity controls to be able to promptly identify cybersecurity breaches.

AI-Platforms and Confidential Data

Employers may also soon face issues involving employees entering confidential information into AI platforms for analysis. One of the benefits of the new AI platforms is their ability to quickly synthesize and summarize data. Yet many of the AI platforms retain users' inputs and may even permit human employees to view these inputs, thereby compromising the confidentiality of this potentially sensitive and, at times, legally protected data. As a result, many companies are already restricting their employees' use of AI platforms to avoid leaks of confidential data. See, e.g., Aaron Tilley and Miles Kruppa, Apple Restricts Employee Use of ChatGPT, Joining Other Companies Wary of Leaks, The Wall Street Journal, May 18, 2023.

To avoid leaking confidential data and the resulting potential activity using that information (including illicit trading), companies should consider using "walled garden" AI systems, whereby the data never leaves their own servers and the employees only use in-house AI. As with the requirement to report hacking, companies should also be proactive in self-reporting any leak of confidential information to the relevant criminal and regulatory authorities.

Risks of AI-Based Trading

As artificial intelligence continues to advance, financial entities will try to leverage it for trading in financial products. Algorithmic trading is already a key part of the markets, and advanced artificial intelligence will likely soon join simpler trading algorithms. In general terms, algorithmic trading differs from AI-based trading because, while an algorithm follows pre-programmed automated instructions, AI is designed to continuously learn and evolve while it performs a task.

But before any financial institution deploys fully automated trading by artificial intelligence, they should be aware of certain potential pitfalls. For example, the Department of Justice and regulators have been closely focused on market manipulation through spoofing and other fraudulent trading strategies by human traders in recent years. See, e.g., United States v. Gregg Smith, Dkt. No. 1:19-cr-00669 (N.D. Ill. 2023) (precious metals trader convicted of market manipulation for alleged spoofing).

Similar to Deep Blue, the supercomputer that famously beat chess Grandmaster Garry Kasparov, it is conceivable that an AI-trading platform may also eventually learn trading strategies, and then engage in legally banned spoofing or other market manipulation, as it seeks advantages in the marketplace.

Along with spoofing and market manipulation, firms employing AI-based trading should also be on the lookout for "wash trading." A wash trade occurs when a trader buys and sells orders to give the appearance that purchases and sales have been made, without incurring market risk or changing the trader's market position.

The CME Group, which operates the Chicago Mercantile Exchange, Chicago Board of Trade, New York Mercantile Exchange, and The Commodity Exchange, has found under its rules that algorithm-generated orders by independent traders will not be considered "wash trades" under certain conditions. Rule 534, Wash Trades Prohibited, CME, Sept. 2, 2020. Algorithmic trades will not be considered "wash trades" if orders are initiated in good faith, the algorithms are operating independently, and the respective trading groups do not have knowledge of the other's orders.

Additionally, firms have an obligation to supervise their employees and their algorithms, and have procedures in place to prevent traders from having knowledge of the other's orders. While many proprietary trading operations that employ algorithms already have "wash protection" built into their algorithms to comply with Rule 534, firms will need to take additional oversight steps to ensure that AI-based trading (that is constantly learning and developing on its own without human input) does not run afoul of wash trading rules or stray into other forms of market manipulation.

FINRA's guidance for companies employing algorithmic strategies provides a helpful jumping off point for firms that may engage in AI-based trading. See FINRA, Algorithmic-based Trading.

Companies should implement a supervision and control program for their AI-based trading with the following characteristics: (i) companies should undertake a holistic review and implement a cross-disciplinary committee to assess and examine risks associated with their AI-based trading; (ii) companies should develop and test their AI-based trading for compliance with the law and to avoid manipulative behavior; (iii) companies should have policies and procedures in place to review their AI-based trading activity once their AI-based trading is active to ensure legal compliance; and (iv) legal and compliance staff at companies must be connected and oversee the employees dedicated to developing and deploying the AI-based trading to ensure continuous compliance with the law.

As AI is continuously learning and adapting, best practices are for companies to engage in regular review of their AI-platforms to ensure continued compliance with the law. Beyond supervision and compliance programs for AI-based trading, companies should also disclose their use of AI-based trading, and be cognizant of the performance of their AI-based trading in comparison to their human traders. The SEC has previously taken a strong stance against allegedly undisclosed algorithmic-based trading that lagged behind its human counterparts. See In the Matter of Bluecrest Capital Mgmt., Securities Act Release No. 10896 (Dec. 8, 2020).

Conclusion

The world is entering a new era with AI. While AI provides new tools for companies, it simultaneously brings with it new avenues for exposure to civil and criminal liability. To leverage the benefits of AI, entities should implement robust compliance and oversight regimes at the outset, and continue to evolve that regime in line with the changing landscape.

Although cybersecurity breaches are inevitable, companies should be ready to disclose such issues as they develop, and, if needed, be in a position to demonstrate to law enforcement and regulators a strong commitment to remediation.

Celia Cohen is a partner in Ballard Spahr's White Collar Defense/Internal Investigations Group, where she represents financial institutions and corporate clients in white collar defense, regulatory compliance, internal and government investigations and related civil actions.

Nathaniel Botwinick is a litigator in the group who represents financial institutions, corporate clients and individuals in government investigations, white-collar defense matters and internal investigations.