GOODWIN

ALERT · OCTOBER 25, 2024

# NYDFS Publishes Guidance on AI-Related Cybersecurity Risks

BY Kaitlin Betancourt L. Judson Welle Peter M. Marta W. Kyle Tayman

On October 16, 2024, the New York State Department of Financial Services (NYDFS or the "Department") published an industry letter (the "Guidance") regarding the increased reliance on artificial intelligence (AI) and the cybersecurity risks associated with that practice.

The Department identified several risks related to legitimate and malicious use of AI and recommended controls and measures to mitigate AI-related risks, including enhancing procedures, technical tools, and training. While the Department notes that the Guidance does not impose new requirements beyond NYDFS's cybersecurity regulation codified at 23 NYCRR Part 500 (the "Cybersecurity Regulation"), the Guidance points to the Cybersecurity Regulation as a framework to assess and address AI-related cybersecurity risks. Entities regulated by the NYDFS ("Covered Entities") would be well-advised to incorporate the Department's guidance into their risk assessments, which is a core component of the Cybersecurity Regulation.

## Risks Related to Malicious AI Use

With respect to malicious use, AI may be leveraged to enhance both the technical and strategic aspects of cyberattacks. The Department highlights that social engineering attacks, which are already prevalent, are becoming more sophisticated. Threat actors may leverage AI tools to create deepfakes, which could allow them to target specific individuals and more easily entice them to divulge sensitive information.

To combat this risk and others posed by AI, organizations should invest in AI cybersecurity training at all levels. This may include procedures adopted by the organization to mitigate risks related to AI and how to respond to AI-enhanced social engineering attacks. In addition, the Cybersecurity Regulation requires that the senior governing body has a sufficient understanding of cybersecurity-related matters, which, according to the Guidance, includes AI-related risks. On a technical level, the implementation of robust access controls is a defensive measure to combat AI-enhanced social engineering attacks. Organizations should consider using an authentication factor that is technologically capable of verifying that the biometric factor comes from a live person. Alternatively, they can use authentication with more than one biometric modality.

There is also risk that the accessibility of AI tools may allow a lower barrier to entry for threat actors, which, in conjunction with AI-enabled deployment speed, has the potential to increase the number and severity of cyberattacks. To combat this risk, organizations should implement effective monitoring to identify new security vulnerabilities promptly so remediation can occur quickly. Organizations must also implement data minimization practices and should maintain and update data inventories, including all information systems that use or rely on AI.

## Risks Related to Legitimate AI Use

In addition, there is increased risk related to the legitimate use of AI. Organizations that use AI tend to collect and process substantial amounts of data, often including nonpublic information (NPI). This creates a greater incentive to target these entities in an attempt to extract NPI for financial gain or other malicious purposes.

Third-party risk is another area of critical concern for organizations using AI. As AI-powered tools depend heavily on the collection of vast amounts of data, the process of gathering that data often involves working with third-party service providers. Any third-party service provider, vendor, or supplier, if compromised by a cybersecurity incident, could expose an entity's NPI and become a gateway for broader attacks on that entity's network as well as all the other networks of entities in the supply chain.

In organizations that use AI, there should be additional controls in place to prevent threat actors from accessing vast amounts of data and to mitigate the risk of supply chain vulnerabilities.

## Risk Assessments and Other Cybersecurity Regulation Components

At the core of the Cybersecurity Regulation is the requirement for a Covered Entity to maintain a cybersecurity program that is based on its risk assessment. The Guidance suggests that the emergence of AI-related cybersecurity risks could constitute, or contribute to, a material change to a Covered Entity's cybersecurity risk such that an update to the Covered Entity's risk assessment may be warranted. The Department recommends designing risk assessments to include both the organization's own use of AI, the AI technologies utilized by third-party service providers and vendors, and any potential vulnerabilities stemming from AI applications.

The Guidance provides that incident response plans should be reasonably designed to address all types of cybersecurity events, including those relating to AI. The Guidance also makes clear that the Cybersecurity Regulation's requirement for the senior governing body to have sufficient understanding of cybersecurity-related matters and to receive and review management reports extends to AI-related risks and matters.

The Department also addresses the following components of the Cybersecurity Regulation in the context of combatting AI-related risks and expounds upon the Department's expectations in each area:

- **Third-Party Service Provider and Vendor Management:** The Guidance stresses the importance of considering the threats facing third-party service providers from the use of AI and the potential impact on the Covered Entity if such threats are exploited. It also provides that, if third-party service providers are using AI, Covered Entities should consider incorporating additional representations and warranties relating to the secure use of NPI.
- **Access Controls:** The Department highlights that multi-factor authentication (MFA) is one of the most effective access controls and includes a reminder to Covered Entities that MFA will be required broadly as of November 1, 2025. Notably, the Department states that AI risks may warrant using authentication factors that can withstand AI-manipulated attacks.
- **Cybersecurity Training:** The Guidance makes clear that cybersecurity training should be enhanced and adjusted to address AI-related risks, in particular with respect to AI-enhanced social engineering attacks (e.g., deepfake attacks).
- **Monitoring:** Covered Entities may need to consider enhanced monitoring to address AI-related risks, including prompt vulnerability management and monitoring the use of AI tools.
- **Data Management:** Covered Entities are reminded to implement data governance procedures that include data collection, storage, processing, and disposal and inventory all systems using AI.

## Key Takeaways

### The Spotlight Is on the Intersection of Cyber and AI

The Department's Guidance places a spotlight on the interrelationship between cybersecurity and AI. While AI presents cybersecurity risks, it also has the potential to provide substantial cybersecurity benefits that can be gained by integrating AI into cybersecurity tools and strategies.

In light of the Guidance, which is largely focused on AI-related risks, Covered Entities should review and reevaluate their cybersecurity programs and controls to account for AI-related cybersecurity risks. Within the Guidance, the Department sets forth specific examples and expectations that should be considered by Covered Entities. For Covered Entities using AI, this may also require a review of the Covered Entity's AI usage and governance. The Guidance concludes by stating that AI-related cybersecurity risks will continue to evolve as AI continues to advance and, therefore, the reevaluation of cybersecurity programs and controls at regular intervals is vital. This stresses the importance of recognizing that compliance with the Department's Cybersecurity Regulation is a complex effort in risk management that requires thoughtful and continuous risk-based consideration.

**Reminder of Impending Deadlines**

The Guidance also serves as a reminder that certain of the more burdensome requirements of the Cybersecurity Regulation have looming deadlines considering the substantial investment of time and resources that may be needed to implement such requirements (implementing MFA broadly and having a comprehensive data inventory are required by November 1, 2025).

**Anticipated Challenges and Suggested Approach**

The Guidance will require companies to undertake efforts that align their governance and risk management processes related to both AI and cybersecurity while factoring in regulatory compliance. Goodwin takes a multidisciplinary approach in helping clients with AI and cybersecurity challenges, which includes drawing on its extensive expertise in cybersecurity risk management, incident response, and cyber-related regulatory advice and litigation defense.

* * *

Please reach out to the authors of this alert or your preferred Goodwin contact for advice related to your specific situation.

*This informational piece, which may be considered advertising under the ethical rules of certain jurisdictions, is provided on the understanding that it does not constitute the rendering of legal advice or other professional advice by Goodwin or its lawyers. Prior results do not guarantee similar outcomes.*

## CONTACTS

### Kaitlin Betancourt
Partner

kbetancourt@goodwinlaw.com
New York | +1 212 813 8936

### L. Judson Welle
Partner

jwelle@goodwinlaw.com
New York | +1 212 459 7400

### Peter M. Marta
Partner

petermarta@goodwinlaw.com
New York | +1 212 813 8048

### W. Kyle Tayman
Partner

ktayman@goodwinlaw.com
Washington, DC | +1 202 346 4245

GOODWIN