NYDFS Issues Letter Highlighting Cybersecurity Risks of AI

October 18, 2024

Alexander H. Southwell | Katelyn N. Ringrose | John C. Ying

SUMMARY

On October 16, 2024, the New York State Department of Financial Services (NYDFS) published a letter to covered entities that calls attention to the risks posed by artificial intelligence (AI). This non-binding guidance letter does not impose any new requirements but instead highlights AI-enabled cybersecurity risks to nonpublic information (NPI) and how certain portions of NYDFS's Part 500 regulations can combat those risks.

This letter is the latest example of NYDFS focusing on and providing guidance related to AI risks. In July 2024, NYDFS published a similar letter highlighting the risks of AI use in insurance underwriting and pricing. And NYDFS's efforts are part of a broader focus in New York to encourage responsible AI development, including Governor Kathy Hochul's focus on AI governance. Below, we summarize the risks NYDFS is concerned about and highlight several key takeaways.

IN DEPTH

RISKS

The letter addresses four central AI-enabled risks that covered entities need to consider if they want an effective cybersecurity program. Two risks arise from threat actors leveraging AI and two from covered entities' use of AI.

Threat Actors Leveraging AI

- *AI-Powered Social Engineering*: With publicly accessible tools that can mimic someone's face, voice, or writing style based on limited samples, it is easier than ever to create deepfake videos, audio, or text that can lead to funds transfer fraud or business email compromise events.
- *AI-Powered Cybersecurity Attacks*: NYDFS points out that threat actors can use AI at every point in the attack chain: deploying malware, mining/exfiltrating NPI, and bypassing security controls. Not only does this increase the speed and scale through which cyberattacks can spread, but it also lowers the barrier to entry for cybercriminals interested in launching attacks through AI code development platforms.

Covered Entities' Use of AI

- *Training Data, Prompts, and Outputs Include NPI*: Developing and deploying AI systems requires a steady flow of training data to build reliable and nondiscriminatory models. This training data can include NPI and, as a result, these systems are significant targets for cyberattacks.
- *Risk of Third-Party Breaches*: Noting that no business can hold, manage, and secure the vast amount of data needed, NYDFS highlighted that particular companies like IT managed service providers, hosting services, and similar services are bigger targets because of the role they play in training and deploying AI systems.

KEY TAKEAWAYS

NYDFS indicates five areas where covered entities should use the framework set forth in Part 500 to assess and address the cybersecurity risks arising from AI:

Conduct Annual Risk Assessments

Part 500.9 requires covered entities to engage in annual risk assessments, which can be expanded to cover AI threats to the business, the business's own use of AI, any third-party AI use, and potential cybersecurity vulnerabilities of these AI systems. These risk assessments should inform other phases of the organization's cybersecurity program, from policies and procedures to tabletop exercises. The process of engaging in a risk assessment can also be a good opportunity for board or senior governing body oversight.

Establish a Third-Party Due Diligence Process

Part 500.11 requires covered entities to implement policies and procedures for how covered entities identify, evaluate, and mitigate cybersecurity threats from third-party vendors they contract with. NYDFS notes how these third-party due diligence efforts can include threats from AI use cases, including having additional representations and warranties related to the secure use of NPI. For example, contracts with vendors employing AI systems could include requirements to abide by certain cybersecurity practices like encryption, multifactor authentication (MFA), and event logging.

Enable MFA for Individuals With Access to NPI

NYDFS also mentions how MFA using at least two of the three authentication factors (something you know, something you have, something you are) is one of the strongest access control methods. Along with previous MFA guidance from 2021, NYDFS recommends that organizations consider how biometric MFA methods can be spoofed with deepfake technology and adjust policies and procedures to account for those risks.

Update Cybersecurity Trainings to Include AI Threats

NYDFS recommends amending employee trainings to address emerging threats and tailoring trainings to employees working with AI systems to ensure they are writing prompts to exclude NPI.

Maintain a Comprehensive Data Inventory

Although not required until November 1, 2026, Part 500.13(a) requires covered entities to maintain and update data inventories. As part of that process, data inventories should identify all AI systems in use by the covered entity and prioritize mitigations based on those systems.

Adding AI considerations onto all Part 500 regulations will require extensive work. For assistance with conducting a risk assessment or analyzing how AI might affect your company's compliance efforts, please contact the authors of this article or your regular McDermott lawyer.

GET IN TOUCH

Alexander H. Southwell
View Profile

Katelyn N. Ringrose
View Profile

John C. Ying
View Profile