PH PRIVACY

NYDFS Issues AI Industry Letter

November 01, 2024
By Aaron Charfoos & Kimia Favagehi

SHARE

On October 16, 2024, the New York Department of Financial Services (NYDFS) issued an industry letter entitled “Cybersecurity Risks Arising from Artificial Intelligence and Strategies to Combat Related Risks” in response to inquiries about how NYDFS covered entities can mitigate risks associated with artificial intelligence (AI). The letter is intended to provide guidance for NYDFS covered entities in assessing AI risks and does not impose any new requirements.

AI-Risks

The letter highlights key risks related to AI, such as AI-enabled social engineering, AI-enhanced cybersecurity attacks, exposure/theft of vast amounts of nonpublic information, and increased third party vulnerabilities. With respect to AI-enabled social engineering specifically, the NYDFS noted that it presents one of the most significant risks to the financial services sector, enabling threat actors to use AI deepfakes to target specific individuals partaking in fraudulent activity.

requires covered entities to assess risks and implement minimum cybersecurity standards designed to mitigate threats relevant to their businesses, *including those posed by AI.* The letter provides several examples of controls and measures that can help entities respond to AI-related risks, which we outline below:

1. **Risk assessments and risk-based programs, policies, procedures, and plans**

   Per the department's guidance, covered entities should assess AI in several areas, including an organization's own use of AI, AI used by vendors, and any possible vulnerabilities stemming from AI technologies that could present significant risks to information systems.

2. **Third-party service provider and vendor management**

   Covered entities should consider the threats facing third-party service providers from the use of AI and how such threats could impact covered entities' business.

3. **Access controls**

   Covered entities are encouraged to employ authentication mechanisms with live detection or texture analysis to verify that a print or other biometric factor comes from a live person. Additionally, effective November 1, 2025, enhanced multi-factor authentication (MFA) requirements will be going into effect requiring a covered entity to have MFA in place for users accessing any information systems containing non-public information, unless alternative controls have been approved by a covered entity's Chief Information Security Officer.

4. **Cybersecurity training**

   Employee training should address the risks presented by AI tools, as well as steps taken by the covered entity to mitigate and respond to such issues. With respect to training specific to cybersecurity personnel, NYDFS notes

5. **Monitoring**

   Covered entities utilizing AI-powered tools should actively monitor such tools for new security vulnerabilities. Additionally, covered entities that use public-facing generative AI platforms should consider monitoring such platforms for strange patterns and behaviors that could indicate an attempt to extract nonpublic information.

6. **Data management**

   Covered entities should have controls in place to prevent threat actors from accessing vast amounts of data maintained for the accurate functioning and training of an AI system. Specifically, covered entities should identify all information systems that use or rely on any AI.

Conclusion

While the NYDFS guidance letter does not impose any new requirements, covered entities subject to the Cybersecurity Regulation should use the letter as a guide to adequately combat risks associated with AI. As AI continues to become more sophisticated, covered entities will need to ensure that they have adequate measures and controls in place to appropriately respond to any resulting risks.

Our Data Privacy and Cybersecurity practice regularly advises on compliance with new AI requirements and guidance, Part 500 Cybersecurity Regulations, and other requirements. If you have any questions concerning how these requirements may affect your organization, please do not hesitate to contact the members of our team.