ALSTON & BIRD

Privacy, Cyber & Data Strategy Advisory: NYDFS Issues Guidance on Artificial-Intelligence-Related Cybersecurity Risks

October 24, 2024

Advisories

By: Kimberly Kiefer Peretti, Katherine Doty Hanniford, Ashley Miller, Lance Taubin, Colton Jackson

On October 16, 2024, the New York Department of Financial Services (NYDFS) issued an industry letter on the cybersecurity risks of artificial Intelligence (AI) and strategies to combat them. The letter contains guidance for entities regulated by the NYDFS in assessing and responding to cybersecurity risks related to the use of AI, specifically its use by threat actors and the risks posed by covered entities' AI systems.

The industry letter does not come as a surprise. The NYDFS previously acknowledged the cybersecurity risks associated with AI in its Assessment of Public Comments (APC) on the revised proposed Second Amendment to 23 NYCRR Part 500, the department's Cybersecurity Regulation, expecting covered entities to take those risks into account in their risk assessments and cybersecurity programs. In the APC, the NYDFS declined to add new sections regarding AI and large language models but indicated this was an area it would continue to monitor.

The letter signaled the NYDFS's interpretation of existing regulations and provided insight into its enforcement priorities. The cyberattack landscape, the NYDFS said, is becoming increasingly more sophisticated by threat actors' use of AI and covered entities' deployment of AI systems and tools.

Risks Posed by AI

In the industry letter, the NYDFS highlights the "most concerning threats" to cybersecurity.

Threat actors' use of AI

The letter discusses numerous risks presented by threat actors' use of AI, including AI-enhanced social engineering, such as phishing attacks and other social engineering schemes using deepfakes. The NYDFS highlights the potential for AI tools to increase the effectiveness, speed, and scale of existing cyberattacks. As we discussed in our October 1, 2024 advisory, the NYDFS reiterated that AI tools can aid in the development of malware and enable less-sophisticated threat actors to conduct increasingly sophisticated and effective cyberattacks.

Inherent risks to AI systems/tools

The NYDFS warns of the potential risks posed by covered entities' use of AI. Inherently, AI systems collect vast amounts of nonpublic information (NPI), making these systems a prime target for threat actors. These risks are particularly strong when AI tools require the storage of biometric data (e.g., facial scans or fingerprints), which threat actors can use to imitate authorized users in order to bypass multi-factor authentication (MFA) protections.

In addition, the collection of these datasets often involves agreements with vendors and third-party service providers (TPSPs), presenting additional links in the chain that can be targeted and compromised by threat actors, potentially exposing sensitive data.

Recommended Controls and Measures to Mitigate AI-Related Threats

With its industry letter, the NYDFS also details extensive recommendations for covered entities to mitigate against the aforementioned risks.

Risk assessments (§ 500.9)

Risk assessments are a foundational requirement under the Cybersecurity Regulation, and the NYDFS has, on multiple occasions, emphasized that risk assessments are a necessary prerequisite to designing and establishing an effective and compliant cybersecurity program. Consistent with the APC's emphasis on the importance of risk assessments' taking into consideration the risks associated with AI (APC, p. 3), the industry letter doubles down, emphasizing that these assessments must now consider risks based on "deepfakes and other threats posed by AI." Also, covered entities should address AI risks stemming from the covered entity's own use of AI, AI used by TPSPs and vendors, and potential vulnerabilities in AI applications.

Incident response and business continuity and disaster recovery plans (§ 500.16)

Covered entities must also maintain incident response (IR) and business continuity and disaster recovery (BCDR) plans designed to address cybersecurity events (as defined in § 500.1(f)) and other disruptions, including those related to AI. We note that the NYDFS clarified in the Second Amendment (and the APC) that "other disruptions" are limited to "cybersecurity-related disruptions," not all disruptive events. It remains unclear how prescriptive a covered entity's IR and BCDR plans must be in addressing AI-imposed risks to cybersecurity events and other disruptions, but it seems that the NYDFS would expect AI to be addressed in those plans in some regard to show the covered entity has considered, or is considering and addressing, the risks posed by AI.

Multi-factor authentication (§ 500.12)

The NYDFS underscored that robust access controls, including MFA (which the NYDFS again singled out as one of the most effective access controls), are important defensive measures to combat the threat of AI-enhanced social engineering, including particularly the threat of deepfakes. The NYDFS uses this industry letter as an opportunity to remind (and perhaps clarify for) covered entities that the enhanced MFA requirements in the Second Amendment come into effect in a little over one year (on November 1, 2025), and MFA must be in place for "all Authorized Users attempting to access Covered Entities' Information Systems or NPI, including customers, employees, contractors, and TPSPs."

Specific to AI, the industry letter encourages covered entities to use authentication factors that cannot be circumvented using AI-enhanced attacks (such as deepfakes), i.e., avoiding SMS text authentication and forms of authentication that can be impersonated by deepfakes, such as voice and video authentication. Instead, the NYDFS promotes the use of digital-based certificates (i.e., a file or electronic password that proves the authenticity of a device or user by cryptography and public-key infrastructure such as a transport layer security certificate) and physical security keys (such as FIDO2 security keys). The NYDFS also encourages covered entities to consider using authentication factors that employ liveness detection technology

or texture analysis, which can help verify if fingerprints or other biometric detection factors come from a live person.

Cybersecurity training

The NYDFS emphasizes the importance of cybersecurity training for all personnel – including, notably, the covered entities' senior executives and senior governing body members – in combating AI-related threats. The NYDFS has emphasized on multiple occasions the importance of cybersecurity awareness training and simulated phishing training and expanded the scope by explicitly adding "social engineering" as an area that must be covered in the cybersecurity awareness training in the Second Amendment. Now, the NYDFS seems to be expanding the training requirement even further, both from a content and a personnel perspective.

- **Cybersecurity Training for All Personnel (§ 500.14(a)(3)).** From a content perspective, the NYDFS suggests incorporating AI-related threats into the cybersecurity awareness training for all personnel to ensure "personnel are aware of the risks posed by AI, procedures adopted by the organization to mitigate risks related to AI, and how to respond to AI-enhanced social engineering attacks." The social engineering component of the training, which can be delivered via simulated phishing and voice and video impersonation exercises, must address deepfake attacks, as well as discussion of procedures for what to do when personnel receive unusual requests typical of social engineering attacks (such as requests for urgent money transfers or access to NPI).
- **Cybersecurity Training for Cybersecurity Personnel (§ 500.10(a)(2)).** As a part of the requirement to provide cybersecurity updates and training sufficient to address relevant cybersecurity risks to all *cybersecurity personnel*, the NYDFS suggests that training should include "how threat actors are using AI in social engineering attacks, how AI is being used to facilitate and enhance existing types of cyberattacks, and how AI can be used to improve cybersecurity."
- **Cybersecurity Training for the Senior Governing Body (§ 500.4(d)).** Interestingly, the NYDFS specifies that it is not just the employees or contractors of the covered entity that must be trained on these AI-related risks (as a part of the broader cybersecurity awareness training) but also the "senior governing body," which is the board of directors (or an appropriate committee, equivalent governing body, or if those do not exist, the senior officer(s). It is atypical for a regulator to prescribe specific cybersecurity training to a board of directors, particularly since the NYDFS removed the requirement from the pre-proposed Second Amendment that the senior governing body have "sufficient expertise and knowledge" of cybersecurity-related matters, replacing it with "sufficient understanding." It would seem, then, that the industry letter suggests that the senior governing body could not have a sufficient understanding of the risks posed by AI without being specifically trained on those risks by the covered entity.

Third-party service provider and vendor management (§ 500.11)

The industry letter notes that covered entities should be mindful of the risks posed to TPSPs by AI and its uses. Covered entities should maintain policies and procedures that ensure due diligence before engaging TPSPs, mandate proper security controls for TPSPs that have access to a covered entity's systems or NPI, and incorporate additional representations and warranties in instances where TPSPs use AI tools. Covered entities should also consider including language in TPSP agreements mandating that TPSPs take advantage of enhanced privacy, security, and confidentiality options when using AI products or services.

Monitoring (§§ 500.5(b) and 500.14)

While the Cybersecurity Regulation already requires covered entities to maintain policies and procedures designed to promptly inform the covered entity of new security vulnerabilities by having a monitoring process in place, as well as a requirement to monitor the activity of users on their system, the NYDFS encourages additional monitoring for covered entities using AI-enabled products, or if they permit personnel to use AI applications such as generative AI applications. This includes monitoring for privacy attacks, which include unusual queries that could indicate attempts to extract NPI. The NYDFS also suggests blocking queries that could expose NPI to a public AI product or system.

Data management (§ 500.13)

The industry letter focuses on the benefits of good data management in reducing the NPI at risk of exposure in the event of system compromise. Covered entities should dispose of NPI that is no longer necessary for business operations or other legitimate business purposes, including NPI used for AI training or other purposes. When maintaining data is necessary for the effective functioning of an AI product or system, covered entities should identify all systems relying on AI-enabled products and prioritize the implementation of mitigations for systems critical to ongoing business operations.

As AI enhances and changes the cybersecurity landscape, the NYDFS also notes the "substantial cybersecurity benefits" of integrating AI into cybersecurity tools – particularly for monitoring systems, analyzing trends, and predicting potential threats. The industry letter suggests that the NYDFS is closely monitoring the AI arms race that continues between threat actors' use of AI to launch cyberattacks and AI-powered cybersecurity defensive tools and, as was the case following prior guidance, may be indicative of the NYDFS's enforcement priorities moving forward.

What Can Companies Do?

- **Revisit education and training materials.** Covered entities should consider reviewing their training materials to update content to educate their personnel and stakeholders as appropriate, including members of the senior governing body, employees, contractors, and TPSPs, on the risks posed by AI, notably the increasingly sophisticated social-engineering and phishing tactics, MFA-bypass techniques, and deepfakes. Cybersecurity tooling is not, and likely will not be, sufficient to guard against the unique risks posed by AI systems, and the use of AI, to launch more sophisticated cyberattacks; cybersecurity awareness training should evolve to address these specific issues.
- **Consider leveraging AI-powered cybersecurity defense tools.** As threat actors continue to use AI to launch cyberattacks, it may become increasingly important to have tools in place aimed at predicting and preventing sophisticated and ever-evolving AI cyberattacks. Cyber defense providers have leveraged AI in their tools, such as endpoint detection and response, for years, but as AI rapidly evolves, covered entities should carefully consider the evolving threat landscape and corresponding cybersecurity defense tooling capabilities to ensure those tools are designed to meet the challenge.
- **Consider phishing-resistant multi-factor authentication when appropriate.** Phishing-resistant MFA can help fortify user accounts against phishing attacks by incorporating multiple layers of protection and applying such advanced techniques as biometric authentication, hardware tokens, and push notifications to trusted devices – adding additional layers of protection to guard against increasingly sophisticated phishing attacks enabled by threat actors' use of AI. Phishing-resistant MFA, such as FIDO2 (a password-less authentication standard allowing users to use either biometric data or a security key), reduces the risks of a threat actor obtaining the unique code sent to the user's mobile device, email account, or mobile app and is now a requirement for federal government agencies (per President Biden's Executive Order 14028).
- **Review/update TPSP agreements and the potential need to consider TPSPs' use of AI.** As AI technology and cybersecurity risks continue to evolve, TPSPs present another link in the chain that could put covered entities' NPI and information systems at risk. In addition to ensuring that new agreements contain language pertaining to AI and data security, companies should consider reviewing and updating old agreements to include these provisions as well. Covered entities should conduct due diligence on TPSPs' use of AI as a part of their periodic TPSP cybersecurity diligence to better understand how the TPSPs are using AI and protecting against the risks posed by AI.

Meet the Authors

Kimberly Kiefer Peretti

Partner

Phone: +1 202 239 3720
Email: kimberly.peretti@alston.com

Katherine Doty Hanniford

Partner

Phone: +1 202 239 3725
Email: kate.hanniford@alston.com

Ashley Miller

Senior Associate

Phone: +1 404 881 7831
Email: ashley.miller@alston.com

Lance Taubin

Senior Associate

Phone: +1 212 905 9301
Email: lance.taubin@alston.com

Colton Jackson

Associate

Phone: +1 202 239 3529
Email: colton.jackson@alston.com