WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

NYDFS Issues Industry Guidance Letter on Artificial Intelligence Cybersecurity Risks

November 1, 2024

AUTHORS

Daniel K. Alvarez | Kara Baysinger | Stephanie Duchene | Matthew J. Gaul
Laura E. Jehl | Susan Rohol | Eun Jung (Michelle) Bae | Elodie O. Currier

On October 16, 2024, the New York Department of Financial Services ("NYDFS") issued a guidance letter outlining cybersecurity risks related to the use of Artificial Intelligence ("AI").[1] While the letter does not impose any new requirements on covered entities,[2] it highlights the ways that AI is changing cyber risks, and directs covered entities to act to address these risks under the requirements of Cybersecurity Regulation 23 NYCRR Part 500 (the "Cybersecurity Regulation"). NYDFS finalized amendments to the Cybersecurity Regulation on November 1, 2023, as discussed in previous Client Alerts here, here, here, and here. A Client Alert on NYDFS's Circular Letter on the Use of AI in Insurance is also available here.

The NYDFS guidance letter clarifies the requirements that the Cybersecurity Regulation imposes on covered entities,[3] including those who do not use AI. In this Client Alert, we highlight these obligations. Covered entities should carefully

[1] The guidance letter is available at https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks.

[2] 23 NYCRR § 500.1(e) defines covered entity as "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies."

[3] We use the term "covered entities" as the NYDFS' guidance letter does, to refer to entities regulated by DFS. Covered entity is defined in 23 NYCRR § 500.1(e) as "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services law, regardless of whether the covered entity is also regulated by other government agencies."

review the guidance letter, consider its implications for deployment of AI in their operations, and assess their cybersecurity postures in response to AI-enabled cybersecurity threats.

Cybersecurity Risks from AI

The guidance letter notes that the financial services sector is a "particularly attractive and lucrative target" for threat actors because of the "maintenance of highly sensitive [Non-Public Information ("NPI")]." NYDFS predicts an increase in the number and severity of cyberattacks on covered entities as AI accelerates the capability and sophistication of threat actors.

First, NYDFS notes a number of ways threat actors can leverage AI, including by using AI in the creation of sophisticated phishing and other social engineering attacks. Attackers can generate realistic and interactive video, audio, or email messages ("deepfakes") that target covered entities' employees.[4] NYDFS notes that these tools can convince employees to take unauthorized actions or divulge NPI, and can mimic an individual's appearance or voice to circumvent biometric verification technologies. We note that with respect to phishing campaigns, AI is a kind of force multiplier—studies have shown that it can reduce the cost to attackers of mounting phishing campaigns by 95%, while maintaining or increasing their success rate.[5]

The guidance letter notes that AI is likely to affect the threat landscape in other ways, including by lowering barriers to entry for less-technologically-sophisticated attackers,[6] accelerating the development of malware and ransomware, and speeding analysis of security vulnerabilities and exfiltration of NPI.

NYDFS is also concerned that covered entities' use of AI products may increase their cybersecurity risk profile. AI products often require covered entities to maintain NPI in large quantities, requiring protection of "substantially more data" and creating a more attractive target for cyberattacks.

Covered entities' use of Third-Party Service Providers ("TPSPs") and other vendors, especially in developing and maintaining AI models, "represents another critical area of concern" for NYDFS. AI model development depends on collection of large volumes of data, often through TPSPs. Any vendor, TPSP, or supplier could therefore provide a gateway for attacks on the covered entity's network. While not discussed in the guidance letter, the National Institute of Standards

[4] FBI San Francisco Division, *FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence*, FBI (May 8, 2024) https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence#:~:text=In%20addition%20to%20traditional%20phishing,their%20way%20to%20their%20employees.

[5] Fredrik Heidig, Bruce Schneier, & Arun Vishwanath, *AI Will Increase the Quantity—and Quality—of Phishing Scams*, Harvard Bus. Rev. (May 30, 2024) https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams.

[6] *Staying Ahead of Threat Actors in the Age of AI,* Microsoft Threat Intelligence (Feb. 14, 2024) https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/#:~:text=Cybercrime%20groups%2C%20nation%2Dstate%20threat,they%20may%20need%20to%20circumvent.

and Technology has also noted that data collection can provide an opening to "poison" an AI model, creating risks that the model will behave in undesirable ways.[7]

Requirements under the Cybersecurity Regulation

The guidance letter emphasizes that the Cybersecurity Regulation's risk assessment and minimum cybersecurity standards include assessment and standards related to AI. In an interview with The Wall Street Journal, NYDFS Superintendent Adrienne Harris emphasized that covered entities need to develop "expertise in the institution, making sure they're engaging with lots of stakeholders, so they understand the development of the technology," even if they do not have internal AI experts.[8] The guidance letter and corresponding NYDFS press release also emphasize the interplay of these requirements to ensure that if one measure fails to mitigate an AI-enabled cyberattack, another safeguard is in place.[9]

Risk Assessments. The guidance letter clarifies that the risk assessment required under the Cybersecurity Regulation must take into account cybersecurity risks, including those posed by deepfakes and other AI threats.[10] It also clarifies that covered entities should design their risk assessments to consider risks related to:

- The organization's own use of AI;
- AI technologies used by third-party service providers and vendors; and

[7] Chad Boutin, *NIST Identifies Types of Cyberattacks that Manipulate Behavior of AI Systems,* Nat'l Inst. Of Standards and Technologies (Jan. 4, 2024) https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems.

[8] Mengqi Sun, *Financial Firms Need to Focus on Cyber Risks Posed by AI, New York Regulator Says,* Wall St. J. (Oct. 16, 2024) https://www.wsj.com/articles/financial-firms-need-to-focus-on-cyber-risks-posed-by-ai-new-york-regulator-says-61c1203d. Prior reporting from The Wall Street Journal indicated that firms have had trouble finding AI-specific experts to fill in-house roles. Catherine Stupp, *Cyber Leaders Struggle to Fill AI Security Jobs,* Wall St. J. (Sept. 20, 2024) https://www.wsj.com/articles/cyber-leaders-struggle-to-fill-ai-security-jobs-8d9a0284.

[9] *See* Press Office, *DFS Superintendent Adrienne A. Harris Issues New Guidance to Address Cybersecurity Risks Arising from Artificial Intelligence*, N.Y. Dep't of Financial Servs. (Oct. 16, 2024) https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20241016.

[10] 23 NYCRR §§ 500.2 and 500.3. Risk assessment is defined in § 500.1(k) as "the risk assessment that each covered entity is required to conduct under Section 500.9 of this Part." Section 500.9 requires that

> Each covered entity shall conduct a periodic risk assessment of the covered entity's information systems to inform the design of the cybersecurity program as required by this Part. Such risk assessment shall be updated as reasonably necessary to address changes to the covered entity's information systems, nonpublic information or business operations. The covered entity's risk assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems.

Risk assessments must be carried out in accordance with written policies and procedures, including "criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the covered entity;" "criteria for the assessment of the confidentiality, integrity, security, and availability of the covered entity's information systems and nonpublic information; including the adequacy of existing controls in the context of identified risks;" and "requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the cybersecurity program will address the risks."

- Vulnerabilities from AI applications that could pose a risk to the confidentiality, integrity, and availability of the Covered Entity's Information Systems or NPI.

These risk assessments must be updated annually and "whenever a change in the business or technology causes a material change to a Covered Entity's cybersecurity risk to ensure new risks, including those posed by AI, are assessed."[11] Risk assessments should determine whether identified risks warrant updates to cybersecurity policies and procedures.[12]

Test Plans. The guidance letter notes that the Cybersecurity Regulation's test plan requirement[13] should be "reasonably designed to address all types of Cybersecurity Events . . . including those relating to AI."

Senior Governing Bodies. NYDFS highlights that the Cyber Security Regulation's requirement that the Senior Governing Body of a covered entity must "have sufficient understanding of cybersecurity-related matters[], exercise oversight of cybersecurity risk management, and regularly receive and review management reports about cybersecurity matters"[14] also includes understanding and oversight of AI-related risks.

TPSP Diligence and Warranties. NYDFS emphasizes the importance of maintaining TPSP policies and procedures that include due diligence before TPSPs are allowed to access a covered entity’s NPI or information systems.[15] The guidance letter “strongly recommends” considering threats to TPSPs from AI and AI products, the TPSP’s security measures and risk mitigation practices, and how threats to the TPSP could impact the covered entity. NYDFS also emphasizes the need for due diligence and contractual protections related to TPSPs, the need for contractual language requiring TPSPs to notify covered entities if a cybersecurity event occurs, and the use of additional representations and warranties related to the secure use of covered entities’ NPI.

Multi-Factor Authentication. The guidance letter recommends the use of multi-factor authentication (“MFA”) and emphasizes that covered entities must require MFA for all authorized users[16] accessing Information Systems or NPI on or before November 1, 2025.[17] NYDFS encourages covered entities to use authentication factors that are hardened against deepfakes and other AI-enhanced attacks, including through the use of digital-based certificates or authentication factors with liveness detection.

[11] Guidance Letter; 23 NYCRR §§ 500.2, 500.3, and 500.9.

[12] Guidance Letter; 23 NYCRR § 500.9(b)(3).

[13] 23 NYCRR § 500.16(a).

[14] Guidance Letter; 23 NYCRR § 500.4(d).

[15] 23 NYCRR § 500.11.

[16] 23 NYCRR § 500.1(b) defines authorized users as “any employee, contractor, agent or other person that participates in the business operations of a covered entity and is authorized to access and use any information systems and data of the covered entity.”

[17] 23 NYCRR § 500.12. As NYDFS emphasized in its December 7, 2021 Guidance on Multi-Factor Authentication, MFA is “a focus of DFS’s cybersecurity supervisory and enforcement work” and is viewed as “essential.” See https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance.

Access Controls. NYDFS also emphasizes that the Cybersecurity Regulation requires covered entities to limit the NPI a threat actor can access if MFA fails to prevent unauthorized access through access controls.[18] These controls must limit an authorized user's access privileges to only those required for their job functions. The Cybersecurity Regulation also requires annual review of access privileges, and imposes requirements for downgrading, terminating, and remote access by authorized users.[19]

Cybersecurity Training. NYDFS emphasizes that the Cybersecurity Regulation requires all personnel, including senior executives and Senior Governing Body members, to receive training on:

- The risks posed by AI;
- Organizational procedures adopted to mitigate AI-related risks; and
- Appropriate response to social engineering attacks, including those conducted with the use of AI. Covered entities must provide at least one annual cybersecurity awareness training that includes social engineering.

If AI is deployed by the covered entity or a TPSP, "relevant personnel" must be trained on:

- Defending and securing AI systems against cybersecurity attacks;
- Designing and developing secure AI systems; and
- Drafting queries to avoid disclosing NPI.

Cybersecurity personnel must also receive AI-related training.[20]

Monitoring. Covered entities must have a monitoring system in place to identify new security vulnerabilities, and must monitor the activity of authorized users, email, and web traffic to avoid cyberattacks.[21] NYDFS encourages covered entities who allow personnel to use AI applications to consider monitoring for unusual query behaviors, and blocking queries that could expose NPI to a public AI model.

[18] 23 NYCRR § 500.7 and 500.12. Footnote 21 of the Guidance Letter also notes that "[w]hile not explicitly required by the Cybersecurity Regulation, best practice is to employ "zero trust" principles, meaning Covered Entities should not implicitly trust the identity of any Authorized User by default."

[19] 23 NYCRR § 500.14(a)(3).

[20] Footnote 26 of the Guidance Letter notes that covered entities may want to consider purchasing commercial cybersecurity awareness training products which include AI-related risk content and incorporate AI to create risk profiles and targeted trainings based on the trainee's knowledge and skill level.

[21] 23 NYCRR § 500.5(b).

Data Management. NYDFS emphasizes that covered entities are required to implement data minimization practices,[22] which must include NPI used for AI purposes. Covered entities must maintain and update data inventories on or before November 1, 2025. NYDFS emphasizes that these data inventories extend to data and information systems affiliated with AI models.

Conclusion

NYDFS' guidance letter confirms that the risks posed by AI-enhanced cyberattacks—including risks associated with the use of AI models—are covered by the Cybersecurity Regulation. It also emphasizes the need for covered entities to actively consider cybersecurity and compliance risk when deploying new AI products, or contracting with vendors who use or provide AI services.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez 202 303 1125 dalvarez@willkie.com	**Kara Baysinger** 415 858 7425 kbaysinger@willkie.com	**Stephanie Duchene** 310 855 3066 sduchene@willkie.com	**Matthew J. Gaul** 212 728 8261 mgaul@willkie.com
Laura E. Jehl 202 303 1056 ljehl@willkie.com	**Susan Rohol** 310 855 3172 srohol@willkie.com	**Eun Jung (Michelle) Bae** 212 728 3166 ebae@willkie.com	**Elodie O. Currier** 212 728 3606 ecurrier@willkie.com

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in Brussels, Chicago, Dallas, Frankfurt, Houston, London, Los Angeles, Milan, Munich, New York, Palo Alto, Paris, Rome, San Francisco and Washington. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

[22] 23 NYCRR § 500.13.