BAKER BOTTS

Thought Leadership

New York State Department of Financial Services Issues Guidance Concerning Cybersecurity Risks Posed by Artificial Intelligence

05 November 2024
Client Updates

Last month, the New York State Department of Financial Services ("DFS"), which has broad regulatory powers over financial services-related entities and insurance companies operating in New York State, published guidance outlining the cybersecurity risks posed by artificial intelligence ("AI"). Although DFS stated that the DFS's guidance (the "Guidance") did "not impose any new requirements" beyond the obligations set forth in its existing cybersecurity regulations, DFS is the latest regulator to weigh in on the measures that companies ought to implement to combat AI-based cybersecurity fraud. Given New York's status as a global financial hub, the Guidance will likely influence how companies beyond the regulatory reach of DFS evaluate their AI-based cybersecurity.

Regulatory Background

Several years ago, in March 2017, DFS first issued cybersecurity regulations (the "Regulations") for entities it regulates ("Covered Entities"). Under the Regulations, a Covered Entity must "assess its specific risk profile and design a program that addresses its risks in a robust fashion." The Regulations also require that senior management annually certify that the Covered Entity's cybersecurity program complies with the Regulations. DFS has amended the regulations over the last several years, and the latest amendments took effect on November 1, 2023. Among the key changes is an updated requirement to perform risk assessments as least once per year as well as "whenever a change in the business or technology causes a material change to the covered entity's cyber risk." The amendment further expands the definition of "risk assessment" to mean:

> the process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, customers, consumers, other organizations and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place.

In addition to updating the Regulations, DFS periodically issues industry guidance; its most recent guidance concerning AI "is meant to explain how Covered Entities should use the framework set forth in [the cybersecurity Regulations] to assess and address the cybersecurity risks arising from AI."

AI Risks

The Guidance highlights four areas of AI-based cybersecurity risk that DFS believes are potential threats to the entities it regulates. The first two risks concern the use of AI by third-party actors to inflict harm on Covered Entities:

- **AI-Enabled Social Engineering**: the deployment of AI by outside actors to "create highly personalized and more sophisticated content" via email, phone or text in an effort to convince Covered Entity employees to divulge sensitive or nonpublic information ("NPI"), provide access to proprietary information systems or facilitate fraudulent transactions to unauthorized or fake accounts.
- **AI-Enhanced Cybersecurity Attacks**: the use of AI by third-party actors to magnify the "scale and speed" of cyberattacks in order more quickly "exploit security vulnerabilities."

The Guidance also notes two areas of risks posed by a Covered Entity's use of AI in the ordinary course of business:

- **Exposure or Theft of NPI**: the integration of AI into any business generally requires the amassing of substantial amount of data, including NPI and biometric data. The mass-collection of this type of sensitive data makes a Covered Entity more susceptible to a cybersecurity attack.
- **Increased Vulnerabilities Due to Third-Party Vendors**: the implementation of AI often requires the support of third-party vendors. DFS cautions that, "[e]ach link in this supply chain introduces potential security vulnerabilities" that bad actors will aim to exploit.

Mitigation Steps Covered Entities Should Consider

Given these risks, DFS provides six examples of controls and measures that Covered Entities—consistent with their obligations under the cybersecurity Regulations—should consider implementing.

- **Risk Assessments**: when designing cybersecurity risk assessments, Covered Entities should factor the evolving AI landscape and tailor their risk assessments both to their own use of AI and that of their third-party intermediaries and vendors. The Guidance further suggests that the plans Covered Entities establish to thwart cybersecurity events "should be reasonably designed to address" threats caused by a third-party actors' use of AI.
- **Third-Party Oversight**: when hiring outside vendors and other third-party providers that will have access to Covered Entities' internal systems and sensitive data, the Guidance recommends that Covered Entities conduct thorough due diligence concerning the third-party providers' ability to withstand AI-based cybersecurity threats. Covered Entities should also review their policies and procedures regarding the level of information access they provide to vendors and should require outside parties to timely report any cybersecurity breach, including those that involve AI.
- **Access Controls**: to combat AI-enhanced attacks, Covered Entities should consider "[i]mplementing robust access controls." In particular, the Guidance urges Covered Entities to use multi-factor authentication, noting that this will be a requirement as of November 2025 for all Authorized Users[1] seeking access to a Covered Entities internal system. Not all authentication factors are created equal and those that can withstand AI-enhanced attacks, such as digital-based certificates and physical security keys, should be favored.
- **Cybersecurity Training**: while the Regulations already mandate that Covered Entities provide cybersecurity training on an annual basis, the Guidance suggests that the training cover the risks posed by AI and the steps that the Covered Entities are taking to mitigate those AI risks. The Guidance further recommends enhanced training for those Covered Entity personnel deploying AI directly to make sure they know how to "secure and defend AI systems from cybersecurity attacks, and how to design and develop AI systems securely."
- **Monitoring**: as with cybersecurity training, while the Regulations require the monitoring of systems for security vulnerabilities and the monitoring of the activity of Authorized Users, the Guidance suggests additional monitoring processes surrounding personnel use of AI applications. Specifically, the Guidance recommends, in the context of AI applications, monitoring for "unusual query behaviors that might indicate an attempt to extract NPI and blocking queries from personnel that might expose NPI to a public AI product or system."
- **Data Management**: for Covered Entities that are using AI or relying on a product that uses AI, the Guidance urges for controls to be put in place to prevent third-party actors "from accessing the vast amounts of data maintained for the accurate function of the AI." Further, the Guidance recommends that Covered Entities "maintain and update data inventories"[2] so that NPI can be readily tracked. In the event of a breach (an AI threat or otherwise), data inventories will allow Covered Entities to know in real time what NPI may have been compromised.

Key Takeaways

Although DFS has imposed cybersecurity requirements for quite some time, the Guidance issued by New York State's financial services regulator demonstrates the need for Covered Entities to closely examine—and refine—their existing cybersecurity policies and procedures in light of the increasing risks posed by AI. Covered Entities should not only take steps to mitigate against the threats of third-party actors using AI to harm their businesses, but they should also take stock of their own use of AI, proactively assessing where vulnerabilities might lie and implementing safeguards to combat those potential areas of weakness. More broadly, the Guidance may serve as a bellwether, impacting how companies beyond the regulatory reach of DFS evaluate and address AI-based cybersecurity risk.

Baker Botts will continue to monitor the regulatory developments in the AI space. If you have questions about this Guidance or how your existing cybersecurity policies and procedures address AI risk, please reach out to any of the lawyers listed below or your usual Baker Botts contact.

Related Professionals

Matthew R. Baker

Partner

Richard B. Harper

Partner

Joseph Perry

Partner

Brendan F. Quigley

Partner

Margaret M. Welsh

Partner