DFS Issues Circular Letter Addressing Cybersecurity Risks Related to AI

OCTOBER 23, 2024

RICHARD G. LISKOV, JULIUS A. ROUSSEAU, III

Share This Page EMAIL LINKEDIN X FACEBOOK

On October 16, the New York Department of Financial Services (DFS) issued a circular letter addressing cybersecurity risks related to the increasing use of artificial intelligence (AI) in relation to insurers, insurance professionals, and banks. These entities must abide by cyberattack regulations, but those regulations have not included any specific requirements related to AI. Although the DFS guidance did not prescribe additional regulations, it detailed the shifting world of cyberattacks and suggested measures firms can take to combat the unique challenges AI poses.

AI Risks

Deepfakes

DFS points to a significant uptick in the amount of cyberattacks involving deepfakes. Deepfakes refer to a type of synthetic video or audio records created with the use of AI that manipulate existing content to make it appear that someone is doing or saying something that they have not. While phishing attacks have been used for decades, deepfakes can make them more effective by making it appear that a request is coming from a trusted person.

For example, earlier this year, a **finance worker at a multinational firm** received an email purporting to be from the firm's CFO discussing the need for a transaction to be carried out. The worker's initial doubts about the authenticity of this request were eased during a video conference call with the CFO and several other employees, where the worker was instructed by the CFO to transfer approximately $25 million. However, what appeared to be a live video of the CFO on that conference call was actually a deepfake. The finance worker instructed to transfer the money was the only real person on the video call.

Other Cyberattacks

Although deepfakes pose a new form of attack, AI also enhances more typical cyberattacks. AI can be used to analyze information, identify security vulnerabilities, and develop a malware variant in a fraction of the time it would take a human to do the same. One concern noted by DFS is how this could increase the number of people capable of carrying out cyberattacks. While attackers once needed to be technologically savvy to carry out these attacks, AI opens the door for those without advanced tech knowledge.

DFS Regulations and Guidance

Under **DFS's Part 500 cybersecurity regulation**, covered entities, such as authorized insurers, are required to conduct periodic assessments of cybersecurity risks, updating the assessment annually and whenever there is a significant change in business or technology that changes the entities' risks. Additionally, entities must maintain a cybersecurity program and policies based on that risk assessment.

Currently, no regulations specifically address the use of AI, but the DFS's guidance instructed entities to consider AI when conducting their risk assessments. Specifically, DFS recommended considering the following factors:

- The entity's own use of AI.
- Third-party service providers and vendors' use of AI — ensuring that policies and procedures address minimum requirement and requiring that the entity is notified of any cybersecurity event.
- Vulnerabilities stemming from AI applications that pose risks to the confidentiality, integrity, and availability of the entity's information systems or non-public information.

In addition to adapting the risk assessment to better identify threats posed by AI, the circular letter gives a number of recommendations, including adopting training on AI threats, implementing robust access controls, and requiring third parties to provide notification of any cybersecurity event. Some of these recommendations are based on regulatory requirements that will go into place in November 2025, but DFS encourages early adoption.[1]

Security Benefits of AI

Despite the known threats of AI as a tool for attacks, DFS acknowledges that AI can also be a security tool. DFS encourages entities to explore using AI for tasks like reviewing security logs, analyzing data, detecting anomalies, and predicting security threats. As technology continues to advance, entities should be mindful not only of the security threats but also how it can be used to enhance security.

ArentFox Schiff is one of the leading law firms for counseling clients on both cybersecurity and AI. Please contact us if we can be of assistance.

[1] As of November 1, 2025, DFS will require multifactor authentication to be used for all authorized users accessing entities' information systems or non-public information. This will not only include employees and third parties, but customers as well. Additionally, entities will be required to maintain data inventories which are used in the identification of risks.

Contacts

Richard G. Liskov

SENIOR COUNSEL

Julius A. Rousseau, III

PARTNER

Related Industries

AI, Metaverse & Blockchain

Insurance & Reinsurance

Continue Reading

ALERTS

The Case for Modernizing Municipal Bond Disclosure Transparency

OCTOBER 23, 2024 | DAVID L. DUBROW

ALERTS

Decades of Regulatory Exemptions Have Been to the Detriment of the Municipal Bond Market

OCTOBER 22, 2024 | DAVID L. DUBROW

ALERTS