June 2025

PH Privacy

NYDFS Urges Covered Entities to Review Security Practices Amidst World Turmoil

By Aaron Charfoos, Michelle A. Reed and Jeremy Berkowitz

Citing "escalating global conflict," the New York Department of Financial Services issued an alert on Monday, June 22, 2025, to its regulated covered entities, urging them to be vigilant against potential security threats, particularly ransomware and phishing attacks. NYDFS recommended covered entities assess their current cybersecurity programs, including by:

1. Testing and updating incident response and business continuity plans, especially the ability to restore backup data.
2. Providing refresher cybersecurity training to employees and contractors, making them aware of recent threats.
3. Reviewing all vulnerability management tools, including endpoint detection protocols, to ensure they are equipped to detect unauthorized activity and new threats.
4. Ensuring that they have robust access management controls in place, particularly around privileged access, operationalizing multifactor authentication and having the ability to disable or secure remote desktop protocol sessions.
5. Reviewing their risk assessments to ensure it aligns with cyber-risk landscape changes.

The alert also reiterated reporting requirements under NYDFS Part 500 Cybersecurity Regulation (to report any security incidents within 72 hours, via the secure Department Portal, which can be accessed from the Cybersecurity Resource Center), as well as notifying relevant law enforcement agencies.

NYDFS issued the alert as companies are also in the final stages of implementing the requirements of the Part 500 amendment that was finalized and approved in November 2023.

Since then, new rules that are part of the amendment have gone into effect in scheduled phases, focused on a number of topics, including: cybersecurity policies; incident response and business continuity plans; security office and board responsibilities; vulnerability management practices; and risk assessment procedures. In November 2025, the final set of rules go into effect, including requirements for:

1. The implementation of multifactor authentication for any individuals accessing any of the covered entities' information systems, unless an entity's chief information security officer approves the equivalent of alternative compensating controls.
2. Maintaining an updated asset inventory that contains key information for all hardware and software assets, including:

    a. Asset owners
    b. Asset locations
    c. Classification of data held on the assets
    d. Asset expiration data
    e. Asset recovery time objectives

Paul Hastings' Data Privacy and Cybersecurity practice regularly advises clients in responding to data breaches and on compliance with Part 500 and other cybersecurity regulations. If you have experienced a breach or have any questions concerning how the changes to Part 500 may affect your organization, please do not hesitate to contact the members of our team listed here.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Chicago	**Dallas**	**Washington, D.C.**
Aaron Charfoos +1-312-499-6016 aaroncharfoos@paulhastings.com	Michelle A. Reed +1-972-936-7475 michellereed@paulhastings.com	Jeremy Berkowitz +1-202-551-1230 jeremyberkowitz@paulhastings.com