Stay Current

PAUL
HASTINGS

March 2026

Follow us on **LinkedIn**

Compliance Update

NYDFS Offers Suggestions on Multifactor Authentication Implementation

By Aaron Charfoos, Michelle Reed and Jeremy Berkowitz

The New York Department of Financial Services (NYDFS) held a webinar on Feb. 26 to provide guidance on the Part 500 Cybersecurity Regulation second amendment's (Part 500) multifactor authentication (MFA) requirements that went into effect last year. The speakers, consisting of NYDFS Cybersecurity Division personnel, provided valuable insights for companies on how they can comply with the new MFA requirements, which we summarize below.

As part of the updated Part 500, which NYDFS amended in 2023, Covered Entities are now required to have MFA in place for individuals accessing "any Information Systems of a Covered Entity." This covers most of the Information Systems of a Covered Entity, with the exception of some public-facing websites. In lieu of MFA, a Covered Entity may alternatively employ the "use of reasonably equivalent or more secure compensating controls" which a Chief Information Security Officer (CISO) must annually review and approve. The second amendment to Part 500 included a number of new requirements that were implemented on a rolling basis over a two-year period, with the MFA requirements taking effect in November 2025. This is the first full calendar year where Covered Entities will need to demonstrate compliance with this requirement, both if they are applying for an NYDFS license and/or recertifying their annual compliance with Part 500.

At the February 26 webinar, speakers reiterated that, under Part 500.01(j), MFA technologies must meet two out of the following three factors:

1. **Knowledge**: Something a user knows (e.g., password or PIN).
2. **Possession**: Something a user has (e.g., a hardware key, mobile authenticator app or smart card).
3. **Inherence**: Something a user is (e.g., fingerprint or facial recognition).

Speakers said they received numerous questions about whether single sign-on (SSO) technology was sufficient to meet MFA requirements. They noted that while SSO can help facilitate authentication, it does not by itself qualify as MFA. Unless your SSO satisfies two of the three factors listed above, it is not sufficient to meet the MFA requirements. Additionally, speakers also emphasized that Third-Party Service Providers, including cloud-based email and document hosting, must also use MFA.

Speakers said that NYDFS personnel will not simply check a box if a Covered Entity says it has MFA in place. They will be examining to see how Covered Entities have implemented MFA and the policies in place to enforce it. They also emphasized the need to focus on solutions that require a more rigorous method than traditional push-based notification (which they believe is less secure), for example by requiring matching pins or challenge response verifications.

NYDFS identified the most common areas of MFA noncompliance:

- Lack of MFA coverage for all systems where required.
- Policy exceptions to waive MFA requirements for certain senior leaders
- Session control gaps for extended periods (longer than 12 or 24 hours) without the need for users to reauthenticate
- Limited monitoring of authentication, particularly anomalous activity and repeated logging attempts

When it comes to implementing compensating controls, the NYDFS in recent months has provided additional insights in the form of frequently asked questions on how it might assess alternatives to MFA, as permitted under 500.12. First, Covered Entities must have a justified written reason for using alternative controls, based on a recent risk assessment conducted by the entity. Second, these alternative controls must be designed to address the same risks MFA was intended to mitigate, such as unauthorized access and potential compromise of system, and not used as a way to get around authentication best practices. Finally, these controls must be tailored to specific systems, so generic controls are unlikely to meet that equivalency.

Paul Hastings' Data Privacy and Cybersecurity practice regularly advises clients on compliance with Part 500 and other cybersecurity regulations. If you 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

Paul Hastings LLP

Stay Current is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership.