Stay Current

PAUL HASTINGS

November 2025

Follow us on LinkedIn

Regulatory Update

NYDFS Puts Third-Party Service Providers Under Regulatory Spotlight

By Aaron Charfoos, Michelle A. Reed and Jeremy Berkowitz

The New York Department of Financial Services (NYDFS) issued an industry letter titled "Guidance on Managing Risks Related to Third-Party Service Providers" (Guidance) for Covered Entities engaging third-party service providers (Service Providers) that process nonpublic information (NPI) under the NYDFS Part 500 Cybersecurity Regulation (Part 500).

While the Guidance explicitly states that NYDFS is not adding any new rules to Part 500, it does clarify existing obligations and potentially signals increased supervisory focus on how Covered Entities should manage Service Provider risks. The Guidance applies to all NYDFS-classified Covered Entities — including Class A Companies and those entities that qualify for a limited exemption under 500.19(a) that use Service Providers which have access to NPI.

Service Provider Due Diligence

NYDFS Part 500.11(a)(3) currently requires Covered Entities to have "due diligence processes used to evaluate the adequacy of cybersecurity practices" of Service Providers, but in the past it has generally not further explained what that due diligence entails. The Guidance provides a "non-exhaustive list" of criteria that can be used to assess Service Providers, including diligence such as:

- Establishing a strong cybersecurity program aligned with standard industry frameworks (e.g., NIST) that is regularly audited through external audits or independent assessments such as ISO/IEC 2700 series or HITRUST.
- Protecting NPI through use of tools such as access controls, multi-factor authentication (MFA), encryption and audit trails.
- Implementing business continuity and incident response plans that are regularly tested.
- Operating in high-risk jurisdictions on geopolitical, legal, socio-economic, operational or other regulatory risks.
- Using robust practices to assess downstream service providers.
- Having a strong reputation in industry along with financial stability.

The Guidance also notes that Covered Entities should consider the criticality of the services provided and the availability of alternative Service Providers in assessing its cybersecurity diligence.

Importantly, the Guidance states that a vendor questionnaire or self-attestation alone is not sufficient to conduct due diligence and that Covered Entities will need to engage with Service Providers to ask follow-up questions and develop mitigation strategies when necessary. In cases in which vendor alternatives are limited or legacy systems restrict vendor choice, Covered Entities should document risk-acceptance decisions, implement compensating controls and regularly reassess whether alternatives have emerged.

Service Provider Contracting

NYDFS 500.11(b) already includes several requirements for Covered Entities to include in contracts with Service Providers, including requiring that Service Providers use MFA and encryption to protect access to NPI, as well as immediately report Cybersecurity Incidents involving NPI.

While not setting new binding contractual obligations, the Guidance identifies additional clauses that Covered Entities should consider in Service Provider contracts including, for example:

- **Compliance Representations:** Service Providers must provide representations and warranties regarding compliance with applicable laws and regulations.
- **Data Location and Transfer Restrictions:** Service Providers should understand where data will be stored and processed and consider cross-border transfer risks.
- **Subcontractors:** Service Providers should disclose their downstream providers that Covered Entities may reserve the right to reject.
- **Data Use and Exit Obligations:** Service Providers should have limitations on use and sharing of data and be required to return or destroy NPI at the termination of contracts.
- **Artificial Intelligence (AI)-Specific Clauses:** If Service Providers use AI for processing NPI, then contracts should address acceptable use of AI and data-training rights.
- **Remedies/Termination Triggers:** Contracts should include rights for Covered Entities to terminate relationships if Service Providers breach cybersecurity provisions.

Service Provider Ongoing Monitoring and Oversight

The Guidance underscores that Service Provider risk management is not a “set-and-forget” exercise but must be ongoing and risk-based. Policies/procedures must mandate periodic reassessment of Service Provider cybersecurity posture relative to risk. Covered Entities should track Service Provider risk management postures including: changes in threat/regulatory environment, changes in the service or system, and any Cybersecurity Incidents experienced by Service Provider. Covered Entities should also consider reviewing attestations/certifications of Service Provider (e.g., SOC 2, ISO 27001), penetration test summaries, audit reports, vulnerability/patching practices and evidence of remedial action. Material or unresolved risks identified in Service Providers relationship should be documented in Covered Entities’ Risk Assessments, escalated to senior governance and incorporated into incident response/business continuity planning.

The Guidance also notes a trend of Covered Entities outsourcing parts or all of their cybersecurity programs to Service Providers or affiliates. It reminds Covered Entities of the importance of maintaining cybersecurity oversight and that they "may not delegate responsibility for compliance with the Cybersecurity Regulation to an Affiliate or a Service Provider." Covered Entities must maintain oversight of Service Providers' activities and ensure they are compliant with NYDFS regulations.

Termination/Onboarding of Service Providers

The Guidance reminds Covered Entities that termination of a Service Provider relationship carries risks and must be managed systematically. Upon termination, Covered Entities should revoke the Service Provider's access to Information Systems and NPI. They should require that Service Providers return or destroy any NPI they still hold, as well as ensure that any snapshots/backups/caches are removed. Covered Entities should also review and document that any redundant access points or lingering privileges have been removed, conduct a final risk review, document lessons learned and incorporate improvements into future arrangements.

Final Amendment Rules Going into Effect

The Guidance comes as Covered Entities are 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 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. On Nov. 1, the final set of rules went into effect, including requirements for:

- The implementation of MFA for any individuals accessing any of the Covered Entities' Information Systems, unless an entity's Chief Information Security Officer ("CISO") approves equivalent alternative compensating controls.
- Maintaining an updated asset inventory that contains key information for all hardware and software assets, including:
  - Asset owners.
  - Asset locations.
  - Classification of data held on the assets.
  - Asset expiration data.
  - Asset recovery time objectives.

Practical Implications for Covered Entities

We recommend that Covered Entities (and their counsel/compliance teams) consider taking the following steps with regard to Service Providers.

- Identify all current Service Providers and categorize them by risk (e.g., access level to NPI, service criticality, geographic/jurisdictional factors).
- Review existing vendor/third-party risk management frameworks, policies and procedures and compare to the phased life-cycle approach articulated in the Guidance.
- Examine current Service Provider contracts for the key provisions highlighted by the Guidance. If absent or inadequate, assess risk and plan contractual amendments or renegotiations for new engagements.
- Develop or refine processes for conducting Service Provider oversight.
- Ensure offboarding protocols are documented, access revocation and data return/destruction procedures are in place and tested, and lessons learned are fed back into vendor risk management.
- Maintain documentation of Risk Assessments, vendor classifying decisions, due-diligence records, contract negotiations, monitoring outcomes, incident responses and offboarding logs.

The Paul Hastings Data Privacy and Cybersecurity practice is closely monitoring these developments. If you have any questions, please do not hesitate to contact any member of our team.

✧ ✧ ✧

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

Chicago

Aaron Charfoos
+1-312-499-6016
aaroncharfoos@paulhastings.com

Dallas

Michelle A. Reed
+1-972-936-7475
michellereed@paulhastings.com

Washington D.C.

Jeremy Berkowitz
+1-202-551-1230
jeremyberkowitz@paulhastings.com