To: The executives and information security personnel at all entities regulated by the New York State Department of Financial Services ("DFS" or the "Department")

Re: Guidance on Managing Risks Related to Third-Party Service Providers

Date: October 21, 2025

Industry Letter

To: The executives and information security personnel at all entities regulated by the New York State Department of Financial Services ("DFS" or the "Department")

Re: Guidance on Managing Risks Related to Third-Party Service Providers

Date: October 21, 2025

Covered Entities[1] have become more reliant on Third-Party Service Providers[2] ("TPSP" or "TPSPs") for services that involve access to Information Systems[3] or Nonpublic Information[4] ("NPI"). Although there are many potential benefits to engaging TPSPs, Covered Entities must understand and address the risks posed by such reliance. For example, reliance on TPSPs introduces the risk of Cybersecurity Incidents[5] at the TPSP, which can have a significant impact on Covered Entities' operations and NPI. Appropriately managing these risks remains a crucial element of a Covered Entity's cybersecurity program.

Covered Entities' exposure to threats will continue to grow as their reliance on technologies managed by TPSPs—such as cloud computing, file transfer systems, artificial intelligence ("AI"), and fintech solutions—increases. The growing scale and complexity of cyber risks posed by TPSPs demands a proactive, risk-based, and continuously adaptive approach to third-party governance. Senior Governing Bodies[6] and Senior Officers[7] must engage actively in cybersecurity risk management, including the oversight of TPSP-related risks.[8] Unless a Covered Entity qualifies for an applicable exemption, Senior Governing Bodies must have a sufficient understanding of cybersecurity-related matters to exercise appropriate oversight, which includes the ability to provide a credible challenge to management's cybersecurity-related decisions to ensure that those decisions align with the entity's overall risk posture and resiliency objectives.[9] The Cybersecurity Regulation ("Part 500") also requires a Senior Officer or the Senior Governing Body to review and approve the Covered Entity's cybersecurity policies and procedures at least annually.[10]

The Department reviews Covered Entities' information security policies and procedures, including those addressing TPSP risk, during examinations and investigations. In these reviews, DFS has identified areas where Covered Entities should strengthen their TPSP programs, including how they monitor, assess, and manage TPSP cybersecurity risk. Specifically, DFS has identified the need for more robust due diligence, contractual provisions, monitoring and oversight, and TPSP risk management policies and procedures. Moreover, DFS has observed a trend in which some Covered Entities outsource critical cybersecurity compliance obligations to TPSPs without ensuring appropriate oversight and verification by Senior Governing Bodies or Senior Officers. As noted in previous guidance, Covered Entities may not delegate responsibility for compliance with the Cybersecurity Regulation to an affiliate or a TPSP.[11] DFS has and will continue to consider the absence of appropriate TPSP risk management practices by Covered Entities in its examinations, investigations, and enforcement actions.[12]

The Department is issuing this guidance on managing risks related to Third-Party Service Providers ("Guidance") to assist Covered Entities of all sizes[13] in addressing risks associated with the use of TPSPs. The Guidance does not impose new requirements or obligations on Covered Entities; rather, it is intended to clarify regulatory requirements, recommend industry best practices to mitigate common risks associated with TPSPs, and promote compliance with relevant sections of Part 500, including Section 500.11.[14] In addition to clarifying regulatory requirements, the Guidance describes steps Covered Entities should consider taking to assess and address cybersecurity risks throughout the lifecycle of a TPSP relationship, beginning with the due diligence and selection processes, continuing through contracting, ongoing oversight and management of the relationship, and ending with the termination of the TPSP relationship.

Identification, Due Diligence, and Selection

When selecting a TPSP, Covered Entities must assess the cybersecurity risks the TPSP poses to the Covered Entity's Information Systems and NPI. Policies and procedures should outline how these risks are evaluated, including minimum cybersecurity standards required for engagement, and procedures for assessing the TPSP's cybersecurity practices and controls based on the unique risks presented by the TPSP.[15]

Covered Entities should classify TPSPs based on the latter's risk profile, considering factors such as system access, data sensitivity, location, and how critical the service provided to the Covered Entity is to its operations. For example, a TPSP with privileged access[16] to a Covered Entity's Information Systems and significant amounts of NPI presents a greater risk than a TPSP that provides services operating outside of the Covered Entity's Information Systems. Providers of critical services that often have a high degree of system-level access and the ability to access sensitive NPI include companies that provide IT managed services, outsourced help desk services, and insurance claims management services.

Additionally, Covered Entities should develop a tailored, risk-based plan to mitigate risks posed by each TPSP. The following is a non-exhaustive list of considerations that Covered Entities should assess when performing due diligence on TPSPs:

- The type and extent of access to Information Systems and NPI.
- The TPSP's reputation within the industry, including its cybersecurity history and financial stability.
- Whether the TPSP has developed and implemented a strong cybersecurity program that addresses, at a minimum, the cybersecurity practices and controls required by the Covered Entity and Part 500.
- The access controls implemented by the TPSP for its own systems and data, as well as to access the Covered Entity's Information Systems, and the proposed handling and storage of Covered Entity data, including whether appropriate controls, such as data segmentation and encryption, are applied based on the sensitivity of the data.[17]
- The criticality of the service(s) provided and the availability of alternative TPSPs.
- Whether the TPSP uses unique, traceable accounts for personnel accessing the Covered Entity's systems and data and whether it maintains audit trails meeting the requirements of Section 500.6.
- Whether the TPSP, its affiliates, or vendors are located in, or operate from, a country or territory jurisdictions that is considered high-risk based on geopolitical, legal, socio-economic, operational, or other regulatory risks.
- Whether the TPSP maintains and regularly tests its incident response and business continuity plans.[18]
- The TPSP's practices for selecting, monitoring, and contracting with downstream service providers ("fourth parties").
- Whether the TPSP undergoes external audits or independent assessments (*e.g.*, ISO/IEC 27000 series, HITRUST) or can otherwise demonstrate, in writing, compliance with Part 500 or industry frameworks such as the National Institute of Standards and Technology's ("NIST") Cybersecurity Framework.[19]

Covered Entities should also consider how best to obtain, review, and validate information provided by prospective TPSPs. For example, a standardized questionnaire may assist in gathering responses, but qualified personnel will need to interpret the responses to make risk-informed decisions, ask follow-up questions as necessary, and determine appropriate mitigation strategies.

In some instances, Covered Entities may face constraints when selecting, contracting with, or transitioning away from a TPSP due to limited vendor options, industry concentration, or legacy system dependencies. In such cases, organizations should make risk-informed decisions, document the relevant risks, take steps to implement compensating controls (*e.g.*, monitoring, segmentation, contract triggers), and conduct regular assessments of the TPSP to evaluate whether viable alternative TPSPs have emerged over time.

Contracting

The Cybersecurity Regulation requires Covered Entities that utilize TPSPs to develop and implement written policies and procedures that address due diligence and contractual protections.[20] These policies must be risked-based and tailored to the services and sensitivity of the data and Information Systems that will be accessed by the TPSP. Below are a few

examples of baseline contract provisions Covered Entities should consider incorporating into their agreements[21] with TPSPs:

- Access Controls – Requirements for TPSPs to develop and implement policies and procedures addressing access controls, including multi-factor authentication, that comply with requirements in Sections 500.7 and 500.12.[22]
- Data Encryption – Obligations to develop and implement policies and procedures addressing encryption in transit and at rest as required by Section 500.15.[23] Although Covered Entities qualifying for exemptions under Section 500.19 are not required to comply with this obligation, given the sensitivity of NPI, such Covered Entities should consider requiring TPSPs encrypt sensitive data, including NPI, in transit and at rest.
- Cybersecurity Event Notification – Provisions related to the immediate or timely notice to the Covered Entity upon the occurrence of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or NPI being held by the TPSP.[24]
- Compliance Representations – Obligations for the TPSP to provide representations and warranties regarding compliance with applicable laws and regulations, including applicable requirements of Part 500.[25]
- Data Location and Transfer Restrictions – Requirements for the TPSP to disclose where data may be stored, processed, or accessed; obtain prior written approval for cross-border transfers (or full prohibitions of this practice); and comply with applicable data residency or localization laws. Although this contractual provision is not explicitly required by the Cybersecurity Regulation, the Department recommends incorporating this provision in contracts because Covered Entities can more effectively analyze the risk to sensitive data, including NPI, when they understand where data is stored and processed.
- Subcontractors – Requirements for the TPSP to disclose the use of subcontractors that may have access to or use the Covered Entity's Information Systems or NPI, as well as the ability of the Covered Entity to reject the use of certain subcontractors for work on its Information Systems or NPI after conducting appropriate due diligence. Although this practice is not required by the Cybersecurity Regulation, the Department recommends adoption of this practice so Covered Entities are better able to analyze the risk to sensitive data, including NPI.
- Data Use and Exit Obligations – Restrictions related to the use and sharing of data, obligations to delete[26] or migrate data held by the TPSP upon termination of the relationship, and obligations to obtain appropriate certifications confirming the completion of these steps.

Where relevant, Covered Entities should consider including a clause related to the acceptable use of Artificial Intelligence ("AI"), and whether the Covered Entity's data may be used to train AI models or be otherwise disclosed to additional parties. In addition, the TPSP agreement should include remedies in the event the Covered Entity reasonably determines that the TPSP has breached any material terms of the agreement related to cybersecurity. These remedies may include requiring timely remediation or permitting early termination of the service agreement.

This is not an exhaustive list of contractual provisions that Covered Entities should consider, nor is this list of terms viable or appropriate in all situations.[27] Covered Entities should carefully

evaluate terms based on the nature of the engagement, market conditions, and the sensitivity of data, among other factors.

Ongoing Monitoring and Oversight

As described above, each Covered Entity's TPSP policy or policies must address, to the extent applicable, the periodic assessment of TPSPs based upon the risk each presents.[28] The TPSP risk management procedures should include layered, risk-informed oversight processes and controls designed to confirm that TPSP cybersecurity programs are aligned with the Covered Entity's cybersecurity expectations.[29] Accordingly, Covered Entities should develop and implement policies and procedures for the ongoing monitoring and oversight of TPSPs. The policies should be informed by a variety of factors, including the evolving threat and regulatory landscape, changes to products and services, and whether the TPSP has experienced a Cybersecurity Event. While many of the initial due diligence considerations remain relevant throughout the relationship, once active, Covered Entities must conduct periodic assessments based on the risk(s) a TPSP presents and the continued adequacy of their cybersecurity practices.[30] These assessments may consider, among other things, security attestations (*e.g.*, SOC2, ISO 27001), penetration testing summaries, policy updates, evidence of security awareness training, and compliance audits.

Moreover, where relevant, Covered Entities should request updates on vulnerability management, assess patching practices, and confirm remediation of previously identified deficiencies. Material or unresolved risk should be documented in the Covered Entity's risk assessment and escalated through appropriate internal risk governance channels. As part of a broader resiliency strategy, Covered Entities should incorporate third-party risk into their incident response and business continuity planning.[31] For example, Covered Entities should assess how they would rapidly transition to alternate systems or providers in the event of a disruption and consider testing relevant portions of their business continuity and incident response plans with their TPSPs.

Termination

When preparing for the end of a TPSP relationship, Covered Entities must disable the TPSP's access to the Covered Entity's Information Systems.[32] This includes revoking system access for TPSP personnel and subcontractors and deactivating service accounts. For TPSPs providing cloud-based services, organizations should revoke identity federation tools (*e.g.*, SSO, OAuth tokens), API integrations, and external storage access. Covered Entities generally should require certification of destruction of NPI, secure return of data to the Covered Entity, or migration of data to another TPSP or internal environment. As part of this process, Covered Entities should confirm that any remaining snapshots, backups, or cached datasets are deleted from TPSP systems and TPSP access to any shared resources is revoked.

Additionally, Covered Entities should give special attention to residual or unmonitored access points that may fall outside routine access provisioning systems. Access points that become redundant or unnecessary during the course of the TPSP relationship should be addressed or

eliminated on an ongoing basis, rather than being left in place until the end of the relationship. Procedures should align with the Covered Entity's cybersecurity program and comply with Section 500.7.

To ensure a secure and orderly termination, Covered Entities should develop a transition plan for critical services with clearly defined timelines, roles and responsibilities. Management should engage key stakeholders, including IT, legal, compliance, procurement, and business units, to identify strategies to mitigate potential risks. Prior to termination, Covered Entities should review the agreement with the TPSP to identify offboarding obligations and protections. In addition, Covered Entities should verify and retain any data subject to legal, regulatory, or litigation hold requirements before initiating data return or destruction processes.

After termination is completed, a final risk review should be conducted to confirm that all obligations have been fulfilled, and that access and data controls have been properly enforced. The offboarding process should be documented and relevant audit logs retained to support accountability and future verification. Finally, any lessons learned should be incorporated into future third-party risk assessments and contracting practices to refine and improve TPSP lifecycle management.

Conclusion

Covered Entities must evaluate and mitigate cybersecurity risks relevant to their own business. To that end, this Guidance highlights risks associated with TPSPs as well as strategies to manage these risks as part of an effective cybersecurity program. As third-party service offerings expand and evolve, so too will TPSP-related cybersecurity risks. Managing these risks appropriately requires performing, at regular intervals, careful analysis of the sufficiency of administrative, technical, and physical controls to manage third-party risk, as required by Part 500.

---

[1] A Covered Entity is defined in § 500.1(e) as "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies." N.Y. Comp. Codes R. & Regs. tit. 23, § 500.1(e) (2025). References to Sections hereinafter refer to those in the Cybersecurity Regulation. Capitalized terms used hereinafter are defined in the Cybersecurity Regulation.

[2] Third-Party Service Provider is defined in § 500.1(s) as "a person that: (1) is not an affiliate of the covered entity; (2) is not a governmental entity; (3) provides services to the covered entity; and (4) maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity."

[3] An Information System is defined in § 500.1(i) as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems."

[4] Nonpublic Information is defined in § 500.1(k) as "all electronic information that is not publicly available information and is: (1) business related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity; (2) any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number; (ii) drivers' license number or non-driver identification card number; (iii) account number, credit or debit card number; (iv) any security code, access code or password that would permit access to an individual's financial account; or (v) biometric records; (3) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to: (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family; (ii) the provision of health care to any individual; or (iii) payment for the provision of health care to any individual."

[5] A Cybersecurity Incident is defined in § 500.1(g) as "a cybersecurity event that has occurred at the covered entity, its affiliates, or a third-party service provider that: (1) impacts the covered entity and requires the covered entity to notify any government body, self-regulatory agency or any other supervisory body; (2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity; or (3) results in the deployment of ransomware within a material part of the covered entity's information systems." A Cybersecurity Event is defined in § 500.1(f) as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system."

[6] A Senior Governing Body is defined in § 500.1(q) as "the board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer or officers of a covered entity responsible for the covered entity's cybersecurity program. For any cybersecurity program or part of a cybersecurity program adopted from an affiliate under section 500.2(d) of this Part, the senior governing body may be that of the affiliate."

[7] A Senior Officer(s) is defined in § 500.1(r) as "the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a covered entity, including a branch or agency of a foreign banking organization subject to this Part."

[8] Tit. 23, § 500.4(d). While Covered Entities that qualify for exemptions under § 500.19 do not need to comply with the requirements of § 500.4, Covered Entities must still maintain a

written cybersecurity policy or policies that are approved at least annually by a Senior Officer(s) or the Senior Governing Body who oversee its implementation. Tit. 23, § 500.3.

[9] *See, e.g.*, Federal Financial Institutions Examination Council Information Technology Examination Handbook, Management Booklet, at I.A.1 *Board of Directors Oversight*, n.3, https://ithandbook.ffiec.gov/it-booklets/management/i-governance/ia-it-governance/ia1-board-of-directors-oversight/ which states that "[a] credible challenge involves being actively engaged, asking thoughtful questions, and exercising independent judgment."

[10] Tit. 23, § 500.3.

[11] *See* N.Y. State Dep't of Fin. Servs., Industry Letter on Adoption of an Affiliate's Cybersecurity Program (Oct. 22, 2021), available at https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211022_affiliates_cybersecurity_program; see also, Bd. of Governors of the Fed. Rsrv. Sys., Fed. Deposit Ins. Corp., Off. of the Comptroller of the Currency, Interagency Guidance on Third-Party Relationships: Risk Management, 88 Fed. Reg. 37920 (June 9, 2023); see also id. tit. 23, § 500.4(a)(1).

[12] See, In the Matter of LifeMark Securities Corporation (2021), available at https://www.dfs.ny.gov/system/files/documents/2021/10/ea20210920_co_lifemark.pdf; see also, In the Matter of OneMain Financial Group, LLC (2023), available at https://www.dfs.ny.gov/system/files/documents/2023/05/ea20230524_co_onemain.pdf.

[13] Note that the Cybersecurity Regulation imposes different requirements on organizations based on their size and resources. See id. § 500.1(d) (describing the qualifying conditions for Class A Companies) and § 500.19(a) (describing the qualifying factors for Covered Entities that are granted limited exemptions based upon the number of Covered Entity personnel, revenue, and assets).

[14] For larger Covered Entities, including Class A Companies, a risk-based approach and solutions may require different steps based upon the unique circumstances, technologies, and other factors relevant to the entity.

[15] Tit. 23, § 500.11(a).

[16] Privileged access refers to the access an Information System user has where the user "is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform." See, definition of a "privileged user," National Institute of Standards and Technology, SP 800-53r5, Appendix A: Glossary, Security and Privacy Controls for Information Systems and Organizations (Sep. 2020, updated Dec. 10, 2020), available at https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[17] Tit. 23, §§ 500.11(b)(1)-(2).

[18] Tit. 23, § 500.16(d).

[19] NIST, The NIST Cybersecurity Framework (CSF) 2.0, available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[20] Tit. 23, § 500.11(b).

[21] The type of agreement, provisions, and exhibits will vary depending on the nature of the services provided and type and breadth of data the TPSP will access. For example, when using cloud-based service providers such as Software-as-a-Service and Infrastructure-as-a-Service, among others, Covered Entities may want to append a service-level agreement, which typically defines service quality expectations, system availability of the product or service for use (commonly referred to as "up-time"), and response and recovery times. Alternatively, organizations providing professional services (e.g., developer, consultant, auditor) generally append Statements of Work to address project-specific obligations, such as deliverables, timelines, and scope. Both documents serve as contractual supplements that clarify roles and expectations under a broader agreement. DFS understands that these types of service-level agreements are often drafted by the TPSP, and that Covered Entities may not always have sufficient leverage to negotiate many of the terms.

[22] Tit. 23, § 500.11(b)(1).

[23] Tit. 23, § 500.11(b)(2).

[24] Section500.11 requires a Covered Entity's policies and procedures to include relevant guidelines covering, among other things, contractual provisions addressing a TPSP's obligation to provide notice of Cybersecurity Events. A Covered Entity's policies and procedures must include guidelines and/or contractual protections that address the notice to be provided in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's NPI being held by the TPSP. See supra note 5 (observing that Cybersecurity Events include more than Cybersecurity Incidents).

[25] Tit. 23, § 500.11(b)(4).

[26] See, e.g., tit. 23, § 500.13(b) (requiring each Covered Entity to have policies and procedures for the secure disposal on a periodic basis of certain NPI no longer necessary for business operations or other legitimate business purposes).

[27] In this circumstance, Covered Entities should still seek to secure reasonable protections, such as breach notification clauses, data use, and assurances regarding access controls and data handling. Additionally, they should consider limiting the volume and sensitivity of data shared, using tokenization to replace sensitive data elements and applying pseudonymization techniques to obscure individual identities, where appropriate. Independent third-party assessments or certifications (e.g., SOC 2, ISO 27001) should also be reviewed and required where feasible. In parallel, organizations should develop medium- to long-term strategies to reduce dependency, such as enabling data portability, modularizing services, or evaluating alternative providers. Moreover, high-risk TPSP relationships should be appropriately escalated through

risk governance frameworks and reflected in the Covered Entity's risk assessments and board-level reporting.

[28] See tit. 23, § 500.11(a)(4).

[29] See, e.g., FINRA, Regulatory Notice 21–29, FINRA Reminds Firms of Their Supervisory Obligations Related to Outsourcing to Third-Party Vendors (Aug. 13, 2021), available at https://www.finra.org/rules-guidance/notices/21-29 (Guidance noting that member firms should consider, among other things, vendor self-assessments, including certified reporting, as well as conducting onsite visits) and NIST SP 800-161r1-upd1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (May 5, 2022, rev. Nov. 1, 2024), available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1-upd1.pdf (Publication recommending that organizations audit Information and Communication Technology "supply chain-relevant events within their information system boundaries" using mechanisms such as system logs, intrusion detection system logs, firewall reports, and other evidence trails.

[30] Tit. 23, § 500.11(a)(4).

[31] See, e.g., tit. 23, § 500.16.

[32] Tit. 23, § 500.7(a)(4).

About Us

State Laws & Regulations

Website

- Accessibility & Reasonable Accommodations
- Disclaimer
- Privacy Policy
- Site Map

Language Assistance

- Language Access Policies and Plans

CONNECT WITH US

- LINKEDIN
- TWITTER
- YOUTUBE