New York Cybersecurity Regulation: Third Party Provisions

Section 500.11 Third Party Service Provider Security Policy.

(a) Third Party Service Provider Policy. Each Covered Entity shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Covered Entity and shall address to the extent applicable:

(1) the identification and risk assessment of Third Party Service Providers;

(2) minimum cybersecurity practices required to be met by such Third Party Service Providers in order for them to do business with the Covered Entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third Party Service Providers; and

(4) periodic assessment of such Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers including to the extent applicable guidelines addressing:

(1) the Third Party Service Provider's policies and procedures for access controls, including its use of Multi-Factor Authentication as required by section 500.12 of this Part, to limit access to relevant Information Systems and Nonpublic Information;

(2) the Third Party Service Provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect Nonpublic Information in transit and at rest;

(3) notice to be provided to the Covered Entity in the event of a Cybersecurity Event directly impacting the Covered Entity's Information Systems or the Covered Entity's Nonpublic Information being held by the Third Party Service Provider; and

(4) representations and warranties addressing the Third Party Service Provider's cybersecurity policies and procedures that relate to the security of the Covered Entity's Information Systems or Nonpublic Information.

(c) Limited Exception. An agent, employee, representative or designee of a Covered Entity who is itself a Covered Entity need not develop its own Third Party Information Security Policy pursuant to this section if the agent, employee, representative or designee follows the policy of the Covered Entity that is required to comply with this Part.

From the NYDFS Cybersecurity Regulation FAQ

2. Can the same entity be a Covered Entity, an Authorized User, and a Third Party Service Provider?

Yes. Depending on the facts and circumstances, the same entity can be a Covered Entity, an Authorized User, and a Third Party Service Provider.

This is common in the case of independent insurance agents. For example, a DFS-licensed independent agent that works with multiple insurance companies is a Covered Entity with its own obligation to establish and maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of its Information Systems and Nonpublic Information. *See* 23 NYCRR 500.02.

In addition, when the independent agent holds or has access to any Nonpublic Information or Information Systems maintained by an insurance company with which it works (for example, for quotations, issuing a policy or any other data or system access), the independent agent will be a Third Party Service Provider with respect to that insurance company; and the insurance company, as a Covered Entity, will be required under 23 NYCRR 500.11 to have written policies and procedures to ensure the security of its Information Systems and Nonpublic Information that are accessible to, or held by, the independent agent (including but not limited to risk based policies and procedures for minimum cybersecurity practices, due diligence processes, periodic assessment, access controls, and encryption).

Further, an independent agent will also be an Authorized User if it participates in the business operations, and is authorized to use any Information Systems and data, of an insurance company that is a Covered Entity. In such a case, the insurance company must implement risk-based policies, procedures and controls to monitor the activities of the independent agent, as more fully described in 23 NYCRR 500.14.

It is also noted that, like any other Covered Entity, an insurance company may also be a Third Party Service Provider and/or Authorized User with respect to another Covered Entity, including an independent insurance agent.

In all events, each Covered Entity is responsible for thoroughly evaluating its relationships with other entities in order to ensure that it is fully complying with all applicable provisions of 23 NYCRR Part 500.

13. If Covered Entity A utilizes Covered Entity B (not related to Covered Entity A) as a Third Party Service Provider, and Covered Entity B provides Covered Entity A with evidence of its Certification of Compliance with NYSDFS Cybersecurity Regulations, could that be considered adequate due diligence under the due diligence process required by Section 500.11(a)(3)?

No. The Department emphasizes the importance of a thorough due diligence process in evaluating the cybersecurity practices of a Third Party Service Provider. Solely relying on the Certification of Compliance will not be adequate due diligence. Covered Entities

must assess the risks each Third Party Service Provider poses to their data and systems and effectively address those risks. The Department has provided a two year transitional period to address these risks and expects Covered Entities to have completed a thorough due diligence process on all Third Party Service Providers by March 1, 2019.

36. Can an entity be both a Covered Entity and a Third Party Service Provider under 23 NYCRR Part 500?

Yes. If an entity is both a Covered Entity and a Third Party Service Provider, the entity is responsible for meeting the requirements of 23 NYCRR Part 500 as a Covered Entity.

37. Are all Third Party Service Providers required to implement Multi-Factor Authentication and encryption when dealing with a Covered Entity?

23 NYCRR 500.11, among other things, generally requires a Covered Entity to develop and implement written policies and procedures designed to ensure the security of the Covered Entity's Information Systems and Nonpublic Information that are accessible to, or held by, Third Party Service Providers. 23 NYCRR 500.11(b) requires a Covered Entity to include in those policies and procedures guidelines, as applicable, addressing certain enumerated issues. Accordingly, 23 NYCRR 500.11(b) requires Covered Entities to make a risk assessment regarding the appropriate controls for Third Party Service Providers based on the individual facts and circumstances presented and does not create a one-size-fits-all solution.