Scott A. Sinder
202 429 6289
ssinder@steptoe.com

1330 Connecticut Avenue, NW
Washington, DC 20036-1795
202 429 3000 main
www.steptoe.com

Steptoe
STEPTOE & JOHNSON LLP

January 8, 2019

TO: The Council of Insurance Agents & Brokers

FROM: Scott A. Sinder
Eva V. Rigamonti
Joshua M. Oppenheimer

RE: **NYSDFS Cybersecurity Rule – Requirements of Third Party Service Providers**

In February 2017, the New York State Department of Financial Services (NYSDFS) published its cybersecurity rule (the "Rule")[1] requiring carriers and agency/brokerage firms, among others, to establish and maintain cybersecurity programs to protect their systems and data. Recent inquiry by Council members into the breadth of the Third Party Service Provider ("TPSP") requirements in the Rule has prompted us to revisit these issues as an addendum to our previously published February 21, 2017 memorandum outlining the overall requirements of the Rule.[2] As described below, TPSPs may have to implement cybersecurity requirements at the request of the Covered Entity they serve that could go *beyond* those required for TPSPs under the Rule, particularly if the TPSP qualifies for one of the Rule's exemptions. A FAQ on this topic reiterates this. The potential for duplication and burdensome requirements as a result of the Rule's circularity is troubling.

Under the Rule, a TPSP will need to comply with the cybersecurity requirements imposed on it by the Covered Entity it serves. To be clear, the TPSP will not be required to comply with its respective Covered Entity's *entire* cybersecurity program, but just those requirements the Covered Entity thinks necessary for the Covered Entity to comply with the

---

[1] New York Department of Financial Services, Final Rule, Cybersecurity Requirements for Financial Services Companies, 23 NYCRR Part 500, *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf.

[2] The February 21, 2017 memorandum (as updated) can be viewed here. Capitalized terms used herein and not otherwise defined have the meanings given to them in the Rule.

Rule's TPSP oversight provisions. Nonetheless, the parameters set by the Covered Entity may require the TPSP (who also is a Covered Entity) to implement cybersecurity requirements *beyond* those required under the Rule. This could very well be the case if the TPSP/Covered Entity qualifies for one of the Rule's exemptions.

The Frequently Asked Question ("FAQ") on this topic merely "clarifies" that TPSPs may have multiple burdensome requirements. In short, TPSPs/Covered Entities may have to essentially duplicate and possibly expand their cybersecurity programs to comply with the requirements imposed on them by their Covered Entities with whom they interact.

The remainder of this memorandum summarizes Covered Entities' TPSP responsibilities under the Rule in further detail. It then breaks down the FAQ addressing this issue, specifically with respect to insurance companies and producers.

I. TPSPs Under the Rule

By March 1, 2019, all Covered Entities[3] must implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information accessible to or held by TPSPs.[4] Such policies and procedures must be based on the Covered Entity's risk assessment and address, to the extent applicable, the identification and risk assessment of these TPSPs, and the minimum cybersecurity practices they must meet before they can do business with the Covered Entity. The risk assessment regarding the appropriate controls for TPSPs must be based on the individual facts and circumstances presented by each TPSP and not created using a one-size-fits-all solution.[5] A Covered Entity must further conduct due diligence and periodic assessments of the adequacy of TPSPs' cybersecurity practices. Simple reliance on a TPSP's Certification of Compliance with the Rule is not adequate due diligence according to NYSDFS,[6] a Covered Entity must actually review the TPSP's cybersecurity practices.

In addition, such policies and procedures must include relevant guidelines for due diligence and/or contractual provisions relating to TPSPs. Those guidelines must address the TPSPs' policies and procedures for access controls, including their use of multi-factor

[3] A Covered Entity is any individual, partnership, corporation, association, or any other entity "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." § 500.01(c), (i) (emphasis added).

[4] § 500.11 (Third Party Service Provider Security Policy). A TPSP is any individual or non-governmental entity that (i) is not an affiliate of the covered entity, (ii) provides services to the covered entity, and (iii) maintains, processes, or otherwise is permitted access to nonpublic information through its provision of services to the covered entity. § 500.01(n) (Third Party Service Provider(s)).

[5] New York State Department of Financial Services, Frequently Asked Questions Regarding 23 NYCRR Part 500 at Question 37, *available at* https://www.dfs.ny.gov/about/cybersecurity_faqs.htm [hereinafter "NYSDFS FAQ"].

[6] *See* NYSDFS FAQ at Question 13 ("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.").

authentication and encryption provided the Covered Entity is non-exempt and thus also subject to these requirements. The guidelines also must address when the TPSP must provide notice 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 that is held by the TPSP. Likewise, the guidelines must specify the representations and warranties necessary for the TPSPs' cybersecurity policies and procedures as they relate to the security of the Covered Entity's systems and information.[7]

To be clear, the Rule does not require the TPSP to comply with the *entire* cybersecurity program of the Covered Entity to which it serves. The TPSP, rather, will need to comply with the cybersecurity parameters imposed on it by the Covered Entity. As a general matter, this will track what is otherwise required by the Rule. However, this may result in a Covered Entity imposing on a TPSP (that also is a Covered Entity) cybersecurity requirements beyond what the Rule requires of that TPSP (due to the TPSP's status as a Covered Entity that is partially exempt).

II. FAQ On Insurance Producer TPSPs

In August 2018, NYSDFS added a FAQ specifically on the status of insurance producers as TPSPs.[8] The FAQ states that a producer may be acting as a Covered Entity, a TPSP, and an Authorized User[9] – all at the same time. As a result, a producer, as a Covered Entity, that also is a TPSP and/or an Authorized User must have a cybersecurity program in place that meets the requirements of the Rule and a cybersecurity program that meets the requirements imposed on it by the insurer(s) it serves as a TPSP and/or as an Authorized User. This may force the producer to create additional or separate compliance structures if its own compliance structure per the Rule does not match the requirements imposed on it by the insurer(s) it serves.

For example, an independent agent working with multiple insurance companies will be considered a Covered Entity with its own obligations to establish and maintain a cybersecurity program.[10] When that independent agent then holds or has access to any Nonpublic Information or Information Systems maintained by an insurance company it serves (e.g., for quotations, issuing a policy, or any other data or systems access), the independent agent will be a TPSP with respect to that insurance company. The insurance company, as a Covered Entity, will be required to have written policies and procedures to ensure the security of its Information Systems and

[7] While covered entities have flexibility to deal with TPSPs, it is unclear how an entity with limited leverage would be able to periodically assess a large vendor's policies.

[8] NYSDFS FAQ at Question 2. *See generally* at Question 36 ("If an entity is both a Covered Entity and a Third Party Service Provider, the entity is responsible for meeting the requirements of [the Rule] as a Covered Entity.").

[9] An Authorized User is any employee, contractor, agent or other individual or non-governmental that participates in the business operations of a Covered Entity and is authorized to access and use any Information Systems and data of the Covered Entity. § 500.01(b) (Authorized User).

[10] § 500.02 (Cybersecurity Program).

Nonpublic Information that are accessible to, or held by, the independent agent (i.e., the TPSP).[11] The independent agent will need to have policies and procedures in place to ensure it can comply with the requirements the insurance company imposes on it, which may be beyond those cybersecurity program requirements imposed on it under the Rule.

Further, an independent agent participating in the business operations, and authorized to use any Information Systems and data, of an insurance company that is a Covered Entity will be considered an Authorized User. The insurance company, as a Covered Entity, will need to implement policies, procedures, and controls to monitor the activities of the independent agent-Authorized User.[12] Again, the independent agent will need to have policies and procedures in place to ensure it can comply with the requirements the insurance company imposes on it. And again, these policies and procedures may be beyond those cybersecurity program requirements imposed on the independent agent under the Rule.

As the above examples illustrate, the NYSDFS interpretation of the Rule essentially requires producers to have their own "first-party" cybersecurity compliance structures that hopefully match the structures imposed on them by the insurers with whom they interact. Compliance with the Rule under this interpretation, therefore, may prove duplicative and burdensome if the producers have to create additional or separate compliance structures to adhere to the different requirements imposed on them by the insurers.

This may very well be the case if the producer qualifies for one of the Rule's exemptions. For example, if a producer qualifies for the "Small New York Business" exemption,[13] it will still need to have a cybersecurity program of its own,[14] but will not need to utilize multi-factor authentication.[15] However, an insurance company that does not qualify for any exemption will need to utilize multi-factor authentication as part of its cybersecurity program, and may find it necessary to require its producers to do the same. A "Small New York Business" exempt producer, therefore, will need to implement multi-factor authentication into its cybersecurity program to meet the requirements imposed on it by the insurance company, even though the Rule does not require it.

[11] § 500.11 (Third Party Service Provider Security Policy).

[12] § 500.14 (Training and Monitoring).

[13] Covered Entities with (1) fewer than 10 employees (including independent contractors) located in New York; (2) less than $5,000,000 in gross annual revenue in each of the prior three fiscal years; or (3) less than $10,000,000 in year-end total assets, qualify for this exemption. § 500.19(a).

[14] § 500.02 (Cybersecurity Program).

[15] § 500.12 (Multi-Factor Authentication).