To: IIABA State Association Executives and Lobbyists

From: Wes Bissett

Subject: New York's Cybersecurity Regulation Service Provider Provisions

As a follow-up to previous discussions concerning the requirements and implications of New York's cybersecurity regulation, we wanted to provide you with further information regarding the third party service provider elements of the rule and how these provisions could possibly affect your members. The effective date of these provisions is quickly approaching, and we suspect that at least some of you are receiving inquiries already. There is considerable confusion and uncertainty surrounding this issue, but this memorandum attempts to provide you with the best information we have at this time. In addition, national is not only working with companies to mitigate the impact of the New York regulation, but also exploring various other advocacy options for agencies affected by this issue.

Executive Summary

What the regulation IS:

- The regulation is expected to have an effect on many insurance agents that do not operate in or are not licensed in New York due to a provision that becomes effective March 1, which requires New York licensees to consider the manner in which nonpublic information is protected by third party service providers, including any insurance agent of a New York-licensed insurer, and to take appropriate action.
- Given the large number of insurers that operate in New York, it is likely that most independent insurance agents across the country will be considered to be a service provider of at least one carrier that has to comply with the rule.

What the regulation IS NOT:

- The regulation does not require New York licensees to compel its service providers to comply with the New York regulation.

Background

Since the passage of the Gramm-Leach-Bliley Act (GLBA) in 1999, all types of financial institutions (including insurers and insurance producers) have been subject to data security requirements and obligations. GLBA directed financial services regulators to establish data security standards, and officials across the various sectors, including insurance, have used this authority to require the implementation of a comprehensive written information security program that includes administrative, technical, and physical safeguards and is appropriate for the size, complexity, and activities of a licensee. These generic provisions have also been interpreted to require licensees to consider the manner in which sensitive information is shared with other parties and to impose appropriate obligations on service providers. Scrutiny of third party service providers by businesses that share sensitive information or provide access to information systems is commonplace and often a critical component of information security programs. See Section VI ("Data Security and Integrity Requirement") of the Gramm-Leach-Bliley Act memo from IIABA's Office of the General Counsel for more information.

The idea that businesses should consider and manage the data risks presented by service providers and vendors is not new, and it is also becoming a marketplace reality as a result of recent experience. The majority of high-profile data breaches that have occurred in recent years were caused by vendors and third parties, and existing requirements and industry standards expect businesses to evaluate service providers and establish appropriate standards. These practices are evident in the insurance industry as well, and the typical agent-company appointment contract already addresses data security. For example, it is becoming more common for carriers to require producers to have a written information security program in place, to provide timely notice of breaches, and to satisfy other obligations, either expressly or through a requirement that agencies comply with all applicable laws and regulations, including data security laws and regulations.

The most notable recent event affecting data security practices in our industry has been the February 2017 adoption of a sweeping, controversial, and poorly crafted cybersecurity regulation by the New York Department of Financial Services (NYDFS). The regulation applies in a direct way to any person that holds a license issued by NYDFS – including all insurers authorized to operate in New York, and all resident and nonresident insurance producers who hold licenses there – and imposes a series of mandates that have taken effect over the last 18 months. Those who hold New York licenses (or "covered entities") are subject to a range of requirements that are outside the scope of this memorandum, but the New York state association has made compliance materials and other helpful information available on its website.

The regulation is also expected to have an effect on many insurance agents that do not operate in or are not licensed in New York due to a final set of requirements that will take effect on March 1. These mandates are found in Section 500.11 and require New York licensees to consider the manner in which nonpublic information is shared with and protected by third party service providers and to take appropriate action. The regulation defines "third party service provider"[1] so broadly that any insurance agent of a New York-licensed insurer is considered to be a service provider of that company for purposes of the rule (even if the agent has no connection to the state). Given the large number of insurers that operate in New York, it is likely that most independent insurance agents across the country will be considered to be a service provider of at least one carrier that is a covered entity under the rule.

While the regulation's service provider provisions could have an impact on agents that do not hold New York licenses, the adverse effects and unnecessary burdens are even greater for those that possess them. This is because NYDFS has indicated that covered entities – including agencies that hold New York licenses – will be expected to scrutinize the data security posture of all carrier partners in addition to more traditional types of vendors and service providers. This may mean that agencies that hold a New York license will, among other things, need to obtain written data privacy assurances from their carriers similar to those that carriers are beginning to require of agents, which will be a significant burden for many resident and nonresident New York licensees.

What Does Section 500.11 Require?

[1] Section 500.01(n) of the regulation defines a "Third Party Service Provider" as "a Person 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."

The obligations that covered entities have vis-à-vis their third party service providers is found in Section 500.11, and the key provisions of that section follow below:

> *(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.*

NYDFS has also provided additional guidance and commentary concerning Section 500.11 in an FAQ document. Several of the questions and answers address third party service provider issues, and we have highlighted some key elements below:

> **Excerpt from FAQ #2** – *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).

Excerpt from FAQ #13 – *The Department emphasizes the importance of a thorough due diligence process in evaluating the cybersecurity practices of a Third Party Service Provider.… Covered Entities must assess the risks each Third Party Service Provider poses to their data and systems and effectively address those risks….*

Excerpt from FAQ #37 – *[Section] 500.11 … 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. [Section] 500.11(b) requires a Covered Entity to include in those policies and procedures guidelines, as applicable, addressing certain enumerated issues … and 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.*

What Does This Mean and What Happens Next?

As you can see, the regulation and the additional guidance do not provide precise direction concerning what a covered entity must do to comply with these vendor risk management requirements. There are no clear-cut obligations, black-and-white mandates, minimum standards, or safe harbors, and many entities are struggling to determine how to comply in an effective and efficient manner. On the other hand, the regulation provides flexibility and enables each covered entity to comply with its own individualized approach.

Although NYDFS has not stated with specificity or clarity exactly what actions a licensee must take vis-à-vis its third party service providers, we wish to note the following:

- The regulation requires the data security policies and procedures of covered entities to address the sharing of any nonpublic information with third party service providers, but the nature of those policies and procedures will be determined by the covered entity's own risk assessment, its risk tolerance, and its views on appropriate data security measures. This means that insurer responses to Section 500.11 will be individualized and may differ. As NYDFS has stated, the regulation requires covered entities to satisfy these obligations "based on the individual facts and circumstances presented and does not create a one-size-fits-all solution."

- As insurers and other covered entities consider what sort of data security standards, contractual requirements, and/or due diligence procedures to put into place, the regulation makes clear that they must at least consider access control and encryption standards and include them to the extent applicable and appropriate. The regulation arguably does not require covered entities to mandate particular access controls (such as multi-factor authentication) or the use of encryption, but it requires these measures to be considered. Covered entities must also address whether and how service providers will be obligated to provide notice of data breaches (something that is already becoming

common in agent-company appointment contracts today) and whether and how vendors might make representations or warranties concerning their data security practices.

- The regulation does **not** require covered entities to compel its service providers to comply with the New York regulation.

- Many agent-company appointment contracts already address many of the issues contemplated by the regulation, either expressly or by requiring agencies to comply with all applicable laws and regulations, including data security laws and regulations, but some New York-licensed insurers are likely to modify their agency contracts in the weeks to come. We have seen a handful of such revisions already, and we have worked with a few insurers on these modifications, which resulted in some improvements being made or considered. While the nature and extent of any contractual amendments or changes in business practices are difficult to predict, we are cautiously optimistic that any carrier responses will be responsible, tailored, and consistent with what is actually required by the regulation. We will continue to work with insurers in various ways to achieve this outcome and limit the impact of the New York regulation on agencies.

Conclusion

We hope this brief memorandum addresses many of the threshold questions that state associations have about the impact of the New York regulation's third party service provider provisions. If you have any questions or concerns about this issue or marketplace activity that is occurring as a result of the regulation, we urge you to contact us.