WSIA WHOLESALE & SPECIALTY INSURANCE ASSOCIATION

4131 N. Mulberry Drive, Suite 200
Kansas City, MO 64116
816.741.3910
F 816.741.5409

NY Cybersecurity Requirements for Financial Services Companies
FAQs

The following answers were provided by Katherine Armstrong of Drinker Biddle, Larry Hamilton of Mayer Brown, John Connell of United Lex and Martin Schwartzman of SBL Solutions during a webinar on August 1, 2017. They are intended for informational purposes only and do not constitute legal advice from the WSIA or any of the participating parties. If you have any questions about the NY Cybersecurity Requirements for Financial Services Companies please consult an attorney.

1. Who within the surplus lines industry is considered a (1) covered entity; (2) affiliate; or (3) both within the meaning of the regulation?

   Larry: Agents and brokers licensed by the NY DFS (including excess line brokers) are covered entities. An affiliate of a covered entity is defined as an entity that controls, is controlled by, or is under common control with a covered entity. Being an affiliate of a covered entity does not make you a covered entity if you are not licensed in New York, but information systems that are shared between covered entities and their affiliates are potentially subject to the New York regulation.

2. How and when are nonadmitted insurers exempt from the regulation and are there situations where they can be linked in as affiliates or third-party service providers?

   Larry: Nonadmitted insurers are not covered entities, but if they are affiliates of covered entities, then the response to question #1 applies. If they are third party service providers to a covered entity, then the obligations that a covered entity has regarding its third-party service providers' cybersecurity will apply to them.

3. Regarding the Wholesale Broker/MGA and Retail Agent relationship, can a Wholesale Broker be considered a Third-Party Service Provider (TSP) of the retailer?

   Larry: If a wholesale broker maintains, processes or otherwise is permitted access to nonpublic information in connection with the services it provides to the retailer, then it is a third-party service provider to the retailer, meaning that the obligations that the retailer has (as a covered entity) with regard to its third-party service providers' cybersecurity will apply to that wholesale broker.

4. Would the regulations and requirements apply to anyone that would have a N.Y. non-resident insurance license?

   Larry: yes, NY DFS licensees are covered entities, whether resident or nonresident.

5. Will certification in accordance with this Regulation be a requirement for licensing renewal?

   Martin: We asked our contacts at the NY DFS, who responded that this has not been considered to date. However, it is possible that DFS may consider such a mechanism in the future.

6. Can brokers that are not NY licensees be made to comply with the regulations or practices by insurers that are impacted by the regulation?

   Larry: If the broker maintains, processes or otherwise is permitted access to nonpublic information in connection with the services it provides to the insurer, then it is a third-party service provider to the insurer, meaning that the obligations that the insurer has (as a covered entity) regarding its third-party service providers' cybersecurity will apply to that broker.

7. For the unlicensed, unauthorized insurer writing business pursuant to the state's excess line laws, are there aspects of this regulation that can still pose exposure and concern that could impose some duty or obligation on the excess line insurer?

   Larry: If the unlicensed, unauthorized insurer is an affiliate of a covered entity and shares information systems with its affiliated covered entity, those systems are potentially subject to the New York regulation.

   Also, it is conceivable that an excess line broker that is a covered entity will regard the excess line insurers with which it deals as its third-party service providers. If an excess line insurer maintains, processes or otherwise is permitted access to nonpublic information in connection with the services it provides to the excess line broker, then it is a third-party service provider to the excess line broker, meaning that the obligations that the excess line broker has (as a covered entity) regarding its third-party service providers' cybersecurity will apply to that excess lien insurer.

8. Are there any exemptions to application of the regulation?

   Larry: See slides 23-26 for an explanation of the exemptions.

9. Regarding the specific exemptions, do they each stand-alone such that a firm that employees 15 individuals, but only has $4.5 million in revenue would be exempt?

   Larry: Yes, you only need to satisfy one of the tests to qualify for the exemption.

10. It seems like there is a little bit of flexibility in the regulations in that in some instances it gives some wiggle room or options, is that true?

    Katherine: There is a lot of specificity for some of the requirements, but flexibility with respect to others. Where the DFS ultimately landed with this regulation is that there is usually no "one-size-fits all" approach, and what may be appropriate for one company is not necessarily appropriate for another company. It is important to understand how your company uses, collects, and handles nonpublic information and that is very fact-specific.

11. Should the surplus lines industry be prepared for more states to implement the same or similar cybersecurity requirements?

    Larry: yes, the NAIC is developing an insurance data security model law and the latest draft is moving closer to the NY DFS cybersecurity regulation.

12. For those that this regulation is applicable, what is the biggest exposure and concern for the surplus lines industry licensee?

    Larry: The biggest exposure and concern is not to take steps to comply with the regulation. The NY DFS recognizes that complying with the many components of the regulation is not a quick and easy process, but you want to be seen as making a diligent effort to comply and put a cybersecurity program in place to protect your nonpublic information, particularly the nonpublic information of your clients.

13. How do we determine if our "Chief Information Security Officer" is qualified?

    Katherine: Section 500.04 provides that the Covered Entity designate a "qualified" individual to be responsible for "overseeing and implementing the CE's cybersecurity program and enforcing its cybersecurity policy." Implicit in that requirement is that the person designated have enough technical expertise to fulfill the role. In our opinion, the NY DFS would likely not question the qualification of the CISO, but will defer to the company's judgment and not second-guess the selection unless it is obvious that the person is not qualified.

14. How does the CISO designation need to be presented to the state in terms of documentation

    Larry: The certification signed by the chairperson of the board or senior officer certifies compliance, but does not identify the CISO. Currently, the covered entity only needs to document the designation of the CISO internally, although it will likely be a checklist item for the triannual examinations.

15. Section 500.10 discusses the need for cyber security personnel training but doesn't say what types of training are required.

    Martin: Section 500.14 sets forth general areas to be covered by training. Based on my experience I find it highly unlikely DFS will mandate the specific content of training but leave it

up to the entity. However, if reviewed on examination I expect DFS to recommend enhancements to the training if it is found not to cover the required broad aspects outlined in the regulation.

16. When creating a Risk Assessment, what specific types of risks should be targeted? How do you best document those results of the assessment? Are companies using outside firms to handle the assessments or have they done it in house?

    Katherine: This will depend in part on what type of nonpublic personal information your company collects and maintains and the data security procedures that are already in place. The purpose of the risk assessment is to inform the development or refinement of the cybersecurity program. Some companies use outside vendors or law firms to handle the assessment. For other companies, the IT department relies on tools which allow them to do the risk assessment in house.

17. Section 500.12 on multifactor authentication – the language says, "may include Multi-Factor Authentication." Is it necessary in all cases or just for remote access as 500.12(b) states?

    Katherine: multi-factor authentication is required for remote access, as 500.12(b) states. In other cases, it may be the most appropriate method, but the regulation does not want to prevent other methods of authentication that could be effective in the particular circumstances.

18. What will be the enforcement mechanism? Will it be part of the triannual examination?

    Martin: we expect enforcement on both the triannual examinations and on compliance reviews by the cyber security unit based upon documentation related to compliance with the regulations. Civil penalties may likely be imposed if noncompliance is discovered and or if inconsistent with the certification on file.

19. Is the online statement through the NY DFS website all that is required to state compliance? Does a written letter need to be sent also?

    Martin: On line compliance statement is sufficient. However, all documents must be made available to DFS upon request or examination.

20. Does non-electronic information fall within the Regulation?

    Larry and Katherine: The definition of nonpublic information only includes electronic information, but if paper records are rendered into electronic form (for example, by being scanned or emailed), then they would become electronic information. Also, bear in mind that state data breach statutes are generally not limited to electronic information.