



New York Cyber Risk Regulations Impose Real Responsibilities on Brokers

By John Dolan
Vice President & Counsel, Government Affairs
The Guardian Life Insurance Company of America (Guardian)

Back in 2017, the State of New York Department of Financial Services (“DFS”) enacted sweeping new cybersecurity regulations that impose real obligations not just on licensed NY insurers, but also licensed NY brokers. The regulations are designed to promote the protection of customer information as well as the information systems of regulated entities. Given the growing number of cybersecurity events, especially directed at financial institutions, DFS concluded that certain regulatory minimum standards were warranted. The intent of these regulations is to not be overly prescriptive but allow entities to use a risk-based approach to address the relevant risks and keep pace with technology advances.

What are my responsibilities?

All NY licensed brokers, such as NY carriers (collectively “Covered Entities”), must:

- Develop a cybersecurity program;
- Develop a cybersecurity policy;
- Meet the access privilege requirements;
- Conduct periodic risk assessments;
- Implement policies relevant to third-party service providers; and
- Limit data retention.

Furthermore, the largest licensed NY brokers that meet certain financial thresholds, like all NY licensed carriers, must also (a) identify a chief information security officer, (b) conduct penetration testing and vulnerability assessments, (c) meet audit trail requirements, (d) meet application security requirements, (e) hire and train cybersecurity personnel, (f) utilize multi-factor authentication, (g) train and monitor employees, (h) encrypt nonpublic information, (i) develop an incident response plan, and (j) notify DFS of a cybersecurity event.

Where do I get more information?

For most NY licensed brokers, if they have not done so already, it will be imperative to proactively apply for a limited exemption to avoid these additional requirements. A broker may apply at the DFS website. To fully understand their obligations, all NY brokers are advised to visit the DFS at <http://www.dfs.ny.gov/about/cybersecurity.htm>.

Will these requirements impact my clients and residents of other states?

It should be noted that the requirements impact all clients of NY licensed brokers, not just those that are situated in or are residents of New York. However, it is expected that DFS is interested in incidents involving or impacting NY residents. Additionally, as of October 2017, the NAIC adopted cyber regulations that generally track these NY cyber regulations, therefore, it is expected that similar requirements will be enacted in other jurisdictions in the coming years.

How is Guardian responding?

Over the past year, Guardian has implemented processes and enhanced our systems to further protect our customer information and meet these requirements. Guardian also is currently assessing the third-party obligations which go into effect in March 2019 and is evaluating changes in our third-party management program that may be needed to fully comply with these requirements.

For Agent/Broker Use Only. Not for Use with the General Public. #2018-56740 (03-20)