Cybersecurity Requirements for Insurance Companies – The NYDFS Rules as the Emerging Standard

August 12, 2020

As we have discussed in recent webinars and blog posts, the New York Department of Financial Services has recently brought its first enforcement action under its cybersecurity rules (23 N.Y.C.R.R. Part 500). When the NYDFS cyber rules were first enacted in 2017, they were widely regarded as the most comprehensive cybersecurity regulation in the United States. Almost all insurance companies that are licensed to do business in New York State were required to comply, leading to speculation that Part 500 would eventually emerge as the cybersecurity standard for insurance companies nationwide. Three years later, that appears to be the case.

Most cybersecurity regimes require companies to meet a certain standard, which is usually to maintain "reasonable cybersecurity," but without specifying any particular measures that must be adopted. For example, California state law requires businesses to maintain "reasonable security procedures and practices…to protect the personal information from unauthorized access…" Similar language appears in the cybersecurity laws of Illinois, Colorado and Louisiana. By contrast, Part 500 details cybersecurity requirements in several specific areas, including personnel, training, policies, access privileges, penetration testing, encryption, multi-factor authentication, application security, data minimization and vendor management.

Before 2018, the FTC had taken a largely standards-based, high-level approach to cybersecurity regulation. But, following the Eleventh Circuit LabMD decision, which criticized the FTC for not providing sufficient clarity to companies as to which cybersecurity measures they must adopt, the FTC has moved more towards a more granular, requirements-based approach to data protection. As we noted in a recent blog post, the proposed amendments to FTC's Safeguard Rule largely track the requirements of Part 500.

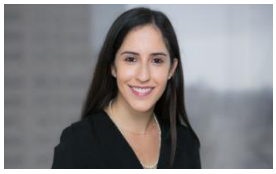
Similarly, the Connecticut Insurance Department recently posted a bulletin containing guidance for insurers as to how to comply with the Connecticut Insurance Data Security Law, which is scheduled to go into effect on October 1, 2020. The Connecticut Insurance Data Security Law was developed based on the NAIC's Model Cybersecurity Law, which closely tracks the specific requirements of the NYDFS rules. Alabama,

Delaware, Michigan, Mississippi, New Hampshire, Ohio and South Carolina have also adopted insurance cyber regulations that are based on the NAIC's model law.

As a result of these developments, thousands of insurance companies are now subject to the specific cyber rules set out in Part 500 or similar regulations. The fact that a large number of these firms have (or soon will) certify their compliance with these rules will make it increasingly difficult for other insurance companies to explain why they have not implemented similar practices, even if not expressly required to do so by regulation. Indeed, it appears that the NYDFS cyber rules may be emerging as the "reasonable cybersecurity" standard for financial institutions, so insurance companies should consider taking a close look at those requirements and evaluating how their existing cybersecurity programs compare.

Luke Dembosky
Partner, Washington, D.C.
+1 202 383 8020
ldembosky@debevoise.com

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com



AJ Salomon
Associate, New York
+1 212 909 6091
asalomon@debevoise.com