KANE RUSSELL COLEMAN LOGAN

One Mission. Your Mission.

New York Cybersecurity Regulations Impacting Financial Services Companies And Their Vendors Are Effective March 1, 2017 And Likely Foreshadow Forthcoming Regulations In Other States.

Banking Law / March 1, 2017 / Jeff Novel

"First-in-the-nation" regulations issued by the New York Department of Financial Services ("NYDFS") which require that financial services companies implement cybersecurity programs are effective March 1, 2017 and will phase in over a period of two years. The NYDFS regulations specifically apply to financial services firms that operate under a license, registration, charter, certificate, permit, accreditation or similar authorization by the NYDFS. The list of affected parties includes banks, credit unions, insurance companies, licensed lenders and loan servicers among other entities ("Covered Entities").

The regulations govern measures relating to cybersecurity which many financial institutions may have already taken such as implementing and maintaining written cybersecurity policies which provide for (1) identification and evaluation of internal and external cybersecurity threats that might compromise nonpublic information stored on the entity's information system; (2) protection of the entity's information system and nonpublic data from unauthorized access through the use of a "defensive structure"; (3) detection of cybersecurity breaches; (4) response to cybersecurity breaches to minimize any adverse impact; (5) recovery from cybersecurity attacks and resumption of normal operations; and (6) satisfaction of all regulatory reporting requirements. However, the regulations also cover areas which may not have been previously addressed by Covered Entities. These potentially uncovered areas include requirements that (1) business-related information be protected in addition to sensitive customer information; (2) Covered Entities appoint a specifically designated Chief Information Security Officer; and (3) an obligation to report certain "Cybersecurity Events," including unsuccessful attempts to access an information system, to NYDFS within 72 hours of any such occurrence.

The new regulations will also affect vendors doing business with Covered Entities in that the new regulations require that Covered Entities adopt 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 must address, to the extent applicable: (1) an identification and risk assessment of third-party service providers; (2) minimum cybersecurity practices required for third-party service providers to do business with the Covered Entity; (3) due diligence processes used to evaluate the adequacy of third-party service providers' cybersecurity practices; and (4) a periodic assessment of third-party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

Although the NYDFS cybersecurity regulations only relate to financial services firms that operate under a license, registration, charter, certificate, permit, accreditation or similar authorization by the NYDFS, as previously noted in this blog, Federal regulators have issued an advanced notice of new proposed cybersecurity standards and other states are likely to implement regulations similar to the cybersecurity standards now required in New York. Financial services

companies should closely watch the evolution of these regulations and start addressing cybersecurity concerns now in order to prepare for forthcoming regulations.

Related Attorneys

Jeff Novel