WINSTON & STRAWN LLP

BLOG

New Cybersecurity Obligations for New York Financial Services Companies

MARCH 22, 2017

The New York Department of Financial Services (NYDFS) recently implemented a new cybersecurity regulation applicable to certain financial services companies—specifically, those authorized to operate under the state's Banking Law, Insurance Law, and Financial Services Law. As in a few other states, covered entities are required to conduct individualized risk assessments and develop written information security policies to address the vulnerabilities identified in the risk assessments. Uniquely, however, New York now requires that covered entities also appoint a senior level employee as Chief Information Security Officer (CISO) to handle cybersecurity matters. Covered entities are also required to notify regulators within 72 hours of certain "cybersecurity events"—in particular, if the event has "a reasonable likelihood of materially harming part of the normal operation(s)" of the covered entity, or if the covered entity is already required to provide notice to another government or supervisory body. Separately, covered entities must implement preventative measures, including an incident response plan, encryption of "non-public" information, multi-factor authentication, and continuous monitoring of company systems (or, in the alternative, periodic penetration testing and bi-annual vulnerability assessments).

The regulation exempts small businesses that meet particular criteria, and certain compliance obligations will be phased in over time. In general, covered entities have 180 days to comply. Certain other requirements take effect one year from the March 1 effective date, including the need to appoint a CISO, conduct a risk assessment, implement multi-factor authentication/penetration testing, and train employees. Other requirements are phased in at the 18-month and two-year mark. Beginning in February 2018, covered entities must provide annual certifications of compliance to state regulators.

TIP: Financial services companies operating in New York and authorized under the New York Banking Law, Insurance Law, and Financial Services Law will need to closely review these regulations (and any potentially applicable exemptions) to determine whether their existing cybersecurity measures meet these new requirements. For example, covered entities will likely need to update their data incident response plans to address these changes.

1 Min Read

Related Locations

Chicago

Related Topics

Financial Privacy

Related Capabilities

Privacy & Data Security | Financial Services Transactions & Regulatory | Financial Services

Related Regions

North America

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.