Special Alert: NYDFS Stakes Claim on Cybersecurity Regulation

On September 13, the New York Department of Financial Services (DFS) issued a proposed rule establishing cybersecurity requirements for financial services companies, and has thus ventured into new territory for state regulators. In the words of Governor Cuomo, “New York, the financial capital of the world, is leading the nation in taking decisive action to protect consumers and our financial system from serious economic harm that is often perpetrated by state-sponsored organizations, global terrorist networks, and other criminal enterprises."

Given the concentrated position of financial service companies in New York and the regulation’s definition of a Covered Entity – which includes “any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law or the financial services law” – it could create an almost de facto national standard for medium to large financial services companies, regardless of where they keep their servers or suffer a cyberattack. This type of state-level regulation is not unprecedented. In 2003, California passed a data breach notification law that requires companies doing business in California to notify California residents of the breach and more recently amended the law to require 12 months of identity protection and strengthen data security requirements. In 2009, Massachusetts enacted a regulation mandating businesses implement security controls to protect personal information relating to state residents.

The DFS designed the regulation to protect both consumers and the financial industry by establishing minimum cybersecurity standards and processes, while allowing for innovative and flexible compliance strategies by each regulated entity. Yet the proposed regulation goes further than to just ask financial entities to conduct a risk assessment and to design measures to address the identified risks.

The regulation contains certain core requirements for financial services companies, including the use of multi-factor authentication, limitations on customer data retention, and encryption of Nonpublic Information, a term broadly defined to include both personal information and confidential sensitive business information. However, the regulation also aims to force Covered Entities to establish certain internal operations and processes. For example, it requires the implementation of a written cybersecurity policy and an incident response plan, both of which are to be overseen and enforced by a Chief Information Security Officer. The regulation also mandates annual penetration testing, limited access to Nonpublic Information (i.e., only to those employees who require access to perform their duties), and cybersecurity awareness training for all personnel.

In addition, the regulation creates particularly stringent obligations for third party oversight, which could be read to require risk assessment and the establishment of cybersecurity standards for all third parties with whom a Covered Entity transacts. The scope of this requirement could be interpreted to be proportionate to the amount of access the third party has to Nonpublic Information, but the regulation is not clear as written. Moreover, the third party oversight requirements may cause friction between Covered Entities and their venders through mandatory contractual requirements, including representations and warranties from the third party service provider and the right to annual audit and review.

The proposed regulation seeks to require notification to the superintendent within 72 hours after a Covered Entity becomes aware of a Cybersecurity Event. The proposed rule defines Cybersecurity Event to include “any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.” Given the increasing number of cyberattacks (of varying levels of sophistication) faced by larger financial services companies, strict adherence to such a requirement could likely lead to an almost endless stream of notification.

Finally, the proposed regulation exempts entities with fewer than 1,000 customers in each of the last three calendar years, less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and less than $10,000,000 in year-end total assets.

* * *

Questions regarding the matters discussed in this Alert may be directed to any of our lawyers listed below, or to any other BuckleySandler attorney with whom you have consulted in the past.

- John P. Kromer, (202) 349-8040
- Elizabeth E. McGinn, (202) 349-7968
- Margo H. K. Tank, (202) 349-8050
- James T. Shreve, (202) 461-2994
- Dana V. Syracuse, (212) 600-2326