Published on *The National Law Review* https://natlawreview.com

Compliance with Initial New York DFS Cybersecurity Rules Now Mandatory

Article By:

Joseph V. Moreno

John T. Moehringer

As of August 28, 2017, insurance companies, banks, and other financial services companies regulated by the New York Department of Financial Services ("DFS") must comply with an initial wave of new cybersecurity requirements intended to protect customer data, including maintaining written cybersecurity policies and procedures, designating a Chief Information Security Officer, and providing notice to the DFS of certain cybersecurity events.[1] Going forward, additional rules will be phased in between the first quarter of 2018 and the first quarter of 2019. Once fully implemented, these "first-in-nation" cybersecurity rules will require not only the adoption of comprehensive cybersecurity programs intended to protect sensitive and confidential data from theft or destruction by cybercriminals, but also the imposition of cybersecurity risk management programs on third party service providers.[2]

Who Is Covered by the Rules?

The new rules apply to "Covered Entities," which include natural persons or businesses "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization" under New York's banking, insurance, and financial services laws.[3] There are, however, certain exceptions and exemptions from the rules, including:

- Branch Offices of U.S. Banks. New York branches of out-of-state domestic banks are *not* required to follow the DFS rules.[4] However, New York branches of foreign banks are required to comply.[5]

- Certain Categories of Covered Entities. Limited exemptions to certain of the DFS rules apply to Covered Entities that (i) have fewer than 10 employees, less than $5 million in gross revenue over the each of the past three years, or less than $10 million in total assets; (ii) are charitable annuity societies under New York Insurance Law § 1110; (iii) do not possess non-public information (as defined by the cybersecurity rules); (iv) are insurance providers not chartered in New York but nevertheless operate within New York, under New York Insurance Law § 5904; or (v) are reinsurers who accept credits or assets from an assuming insurer not authorized in New York.

Which Provisions Are Now Mandatory?

As of August 28, 2017, Covered Entities must comply with the following provisions:

- Implement a Cybersecurity Program. Covered Entities must implement a cybersecurity program and adopt written cybersecurity policies and procedures, including an incident response plan. The policies and procedures must be approved by the board or senior management, and must be risk-based and tailored to the specific business model and risk profile of the Covered Entity.

- Designate a Chief Information Security Officer. Covered Entities must designate a qualified Chief Information Security Officer and retain cybersecurity personnel who stay up-to-date with the latest cyber threats and countermeasures.

- Conduct Periodic User Access Assessments. Covered Entities must periodically review who has access to the Covered Entity's confidential data and computer networks and place appropriate limitations on that access.

- Report Breach Incidents. Covered Entities must report to the DFS within 72 hours any "cybersecurity event" when *either* (i) there is a pre-existing duty to notify a separate government body or regulatory agency of a cybersecurity event (such as, for example, a duty to report to state regulators under New York data breach notification laws), or (ii) the cybersecurity event at issue has a reasonable likelihood of materially harming any part of its normal operations. According to supplemental guidance issued by the DFS, Covered Entities are required to report even unsuccessful cybersecurity attacks when, in the judgment of the covered entity, such attacks are "sufficiently serious to raise a concern." The DFS has created a secure portal for filing notices, available at http://www.dfs.ny.gov/about/cybersecurity.htm.

What Else Is Coming?

Additional requirements under the DFS rules will become mandatory over the course of the next two years, including obligations to certify compliance and mandates for Covered Entities to adopt specific technological solutions for cybersecurity, such as two-factor authentication. Relevant dates include:

- February 15, 2018: Covered Entities must begin making annual compliance certifications to the DFS, signed by the board or a senior officer.

- March 1, 2018: Covered Entities must implement multi-factor authentication, undertake regular penetration testing and risk assessments, and implement cybersecurity awareness training for staff.

- September 1, 2018: Covered Entities must encrypt confidential data in transit over external networks and at rest, monitor user activity, implement secure data disposal procedures, and maintain audit trails of network activity and significant transactions.

- March 1, 2019: Covered Entities must adopt comprehensive cybersecurity risk management programs for third party service providers.

Conclusion

DFS Commissioner Maria Vullo has declared cybersecurity to be a high priority, vowing that "[r]egulated entities will be held accountable" for failing to safeguard customer information.[6] Failure to comply will place Covered Entities – and, potentially, their employees, managers, and directors – at risk of enforcement actions and penalties. As a result, insurance companies, banks, and other financial services companies regulated by the DFS should consult with counsel regarding their cybersecurity programs in light of these strict new rules.

---

1 *See* New York Department of Financial Services, Cybersecurity Requirements for Financial Services Companies (Mar. 1, 2017), 23 N.Y.C.R.R. Part 500, *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

2 *See* Cadwalader Clients & Friends Alert, *New York State Releases Final "First-in-Nation" Cybersecurity Rules* (Feb. 28, 2017), *available at* http://www.cadwalader.com/uploads/cfmemos/4944e3e468c5f24b20e5f3c7e07135a0.pdf.

3 *See* 23 N.Y.C.R.R. Part 500 § 500.01(c).

4 *See* New York Department of Financial Services, Frequently Asked Questions Regarding 23 NYCRR Part 500 (updated Sept. 6, 2017), *available at* http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

5 *See id*.

6 *See* Press Release, *Governor Cuomo Announces Proposal of First-in-the-Nation Cybersecurity Regulation to Protect Consumers and Financial Institutions* (Sept. 13, 2016), *available at* http://www.dfs.ny.gov/about/press/pr1609131.htm.

National Law Review, Volume VII, Number 255

Source URL:https://natlawreview.com/article/compliance-initial-new-york-dfs-cybersecurity-rules-now-mandatory