KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

February 9, 2018

NY DFS Regulation: Certify Your Compliance by February 15 and Assess Your Risk by March 1

The New York Department of Financial Services' (DFS) cybersecurity regulation (DFS Regulation), which took effect on March 1, 2017, imposes significant requirements on financial services companies doing business in New York. Covered entities are likely already familiar with much of the rule, as the first transitional period ended on August 28, 2017 (see our previous client alert for a summary of compliance steps). By February 15, 2018, covered entities must submit their first annual certification of compliance with the regulation.[1] Also around the corner is the deadline for additional required steps, such as completing a risk assessment and implementing multi-factor authentication. In-house counsel should ensure that those compliance steps are taken by the end of the second transition period on March 1, 2018.

Even companies that are not subject to the DFS Regulation would do well to get out ahead of the issue, since the trend of industry-targeted cybersecurity regulation seems likely to continue. In September 2017, Governor Andrew Cuomo directed the DFS to increase the scope of the DFS Regulation to apply to credit reporting agencies,[2] which must now register with DFS and comply with the DFS Regulation. Cybersecurity experts expect that that other regulatory and law enforcement agencies will look to the DFS Regulation in developing their own cybersecurity regulations.

Certify Compliance by February 15, 2018

It is time for all "Covered Entities"—entities and individuals supervised by the Department of Financial Services—to certify their compliance with the DFS regulation. All entities must submit their first annual Certificate of Compliance this month.[3] The Board of Directors or other senior officer of the Covered Entity must certify that the entity's cybersecurity program complies with the DFS Regulation. These Certifications of Compliance can be filed electronically on the DFS website.[4] Note that Covered Entities cannot rely on an affiliate's certification: each entity is required to annually certify its own compliance with Part 500. A subsidiary cannot rely on its parent company's certification.[5]

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Anush Emelianova
+1 404 572 4616
aemelianova@kslaw.com

Kyle A. Brown
+1 212 556 2287
kabrown@kslaw.com

King & Spalding

www.kslaw.com

Implement Second Transition Period Requirements by March 1, 2018

When the one year transition period ends on March 1, all Covered Entities must also implement the following requirement:

- **Risk Assessment** (23 NYCRR 500.09): All Covered Entities must conduct a written risk assessment by March 1. This assessment must be performed again if there is a material change to any of the aspects addressed by the assessment.

Unless subject to the limited exemption[6] for smaller entities, Covered Entities must also implement the following requirements by March 1:

- **CISO Reporting** (23 NYCRR 500.04(b)): Annually and in writing, the Chief Information Security Officer must report on the Covered Entity's cybersecurity program and material cybersecurity risks to the covered entity's Board.

- **Penetration Testing and Vulnerability Assessments** *or* **Continuous Monitoring** (23 NYCRR 500.05): Covered Entities must assess their cybersecurity programs in one of two ways: (1) conduct annual penetration testing and biannual vulnerability assessments in accordance with its risk assessment, or (2) implement "continuous monitoring," which means monitoring that is "effective" and detects "ongoing" changes that may create vulnerabilities. DFS has clarified that "non-continuous monitoring of Information Systems, such as through periodic manual review of logs and firewall configurations" does not qualify.[7]

- **Multi-Factor Authentication** (23 NYCRR 500.12): Covered Entities must use multi-factor authentication, or a reasonably equivalent alternative, when individuals access internal networks from an external network and to protect against unauthorized access.

- **Cybersecurity Awareness Training**: (23 NYCRR 500.14(b)): All personnel must receive regular cybersecurity awareness training that is updated per the risk assessment.

Upcoming Transition Periods Ending September 3, 2018 and March 1, 2019

By September 3, 2018, Covered Entities must have drafted written procedures detailing secure software development practices and policies to prevent internal authorized users from tampering with nonpublic information. Covered Entities must also maintain audit trails for five years, encrypt nonpublic information, and dispose of nonpublic information securely. By March 1, 2019, Covered Entities must develop cybersecurity policies regarding data held by third party service providers. Covered Entities will have to certify their compliance with the regulation yearly, and may benefit from a compliance review prior to certification.

King & Spalding's Data, Privacy & Security Practice

With more than 60 Data, Privacy & Security lawyers in offices across the United States, Europe, and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and cybersecurity-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy. Our Data, Privacy & Security Practice has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data

breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

[1] 23 NYCRR 500, *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.
[2] 23 NYCRR 201, *available at* http://www.dfs.ny.gov/legal/regulations/proposed/propdfs.htm.
[3] 23 NYCRR 500.17(b), Appendix A.
[4] New York Department of Financial Services, *Key Dates under New York's Cybersecurity Regulation (23 NYCRR Part 500)*, http://www.dfs.ny.gov/about/cybersecurity.htm (Sept. 27, 2017).
[5] See 23 NYCRR 500.01(a) (if an entity controls the policy of another entity, they are affiliated).
[6] 23 NYCRR 500.19 exempts entities with "(1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates located in New York or responsible for business of the Covered Entity, or (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or (3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates…" and those that do not "directly or indirectly control, own, access, generate, receive, or possess Nonpublic Information."
[7] New York Department of Financial Services, *Frequently Asked Questions Regarding 23 NYCRR Part 500*, http://www.dfs.ny.gov/about/cybersecurity_faqs.htm (Dec. 12, 2017).