KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

August 8, 2017

And So It Begins: The First DFS Transition Period Comes to an End August 28

In September 2016, the New York Department of Financial Services ("DFS") introduced the first draft of its cybersecurity regulation,[1] which is now in a position to lead a new trend in industry-specific cybersecurity regulation. The regulation contains detailed and demanding requirements that require increased executive and senior management participation in cybersecurity, comprehensive risk analyses, written policies and procedures, specific technical safeguards, and annual compliance certifications for companies in the financial services industry. The regulation became effective as of March 1 of this year and provides various transition periods, including 180 days to comply with core requirements, one year to implement risk vulnerability testing, eighteen months to implement application security and encryption policies, and two years to contractually require service providers to maintain adequate cybersecurity policies. On August 28, 2017, the first transition period ends and covered entities will be required to comply with several of the regulation's exacting requirements. Here is what in-house counsel should know about the first transition period.

Does My Company Need to Comply With the Regulation?

Generally, covered entities under the cybersecurity regulation include all individuals and entities directly supervised by DFS and may include those entities' service providers.[2] Certain smaller entities may qualify for a limited exemption, but in order to be exempted, those entities must submit a Notice of Exemption[3] on or before September 27, 2017. Exempt entities,[4] which are generally small businesses, remain subject to the regulation's core requirements described below.

What are the August 28 Compliance Requirements?

All covered entities must implement the following requirements by August 28, 2017:

- **Cybersecurity Program** (23 NYCRR 500.02) – the program should be designed to protect the confidentiality, integrity, and availability of the entity's information systems and informed by the entity's risk assessment. Key areas of focus for the required cybersecurity program include:

For more information, contact:

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

Nicholas A. Oldham
+1 202 626 3740
noldham@kslaw.com

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

www.kslaw.com

- Identify and assess cybersecurity risks;
- Protect information systems through defensive infrastructure and policies;
- Detect Cybersecurity Events;[5]
- Respond to and mitigate the effects of Cybersecurity Events;
- Recover from Cybersecurity Events; and
- Fulfill regulatory reporting obligations.

- **Cybersecurity Policy** (23 NYCRR 500.03) – the policy should be a written document, or collection of documents, that sets forth the policies and procedures for the protection of the entity's information systems and nonpublic information and is approved by the entity's senior management. The policy should be based on the entity's risk assessment and cover 14 enumerated areas related to data privacy and cybersecurity issues.

- **Access Privileges** (23 NYCRR 500.07) – implement user access privileges to limit access to Nonpublic Information[6] based on risk assessment.

- **Notices to Superintendent** (23 NYCRR 500.17) – covered entities must notify the Superintendent of Cybersecurity Events which require notification to another regulatory or self-regulatory body, or that have a reasonable likelihood of materially harming operations within 72 hours of determining that such an Event has occurred.

In addition, covered entities *not subject to the limited exemption* must implement:

- **Chief Information Security Officer** (23 NYCRR 500.04 (a)) – each covered entity must designate a qualified CISO who is responsible for overseeing the cybersecurity program and enforcing the cybersecurity policy. The CISO role may be outsourced with appropriate supervision by the covered entity.

- **Personnel and Intelligence** (23 NYCRR 500.10) – covered entities must use qualified personnel to manage cybersecurity risks and oversee performance of the core program functions. The covered entity must ensure personnel are provided with sufficient training and take appropriate steps to maintain knowledge of current cybersecurity threats and countermeasures.

- **Incident Response Plan** (23 NYCRR 500.16) – covered entities must have in place a written response plan designed to respond to and recover from material Cybersecurity Events. The plan should address the following seven areas: (1) the internal processes for responding to a Cybersecurity Event; (2) the goals of the incident response plan; (3) the definition of clear roles, responsibilities and levels of decision-making authority; (4) external and internal communications and information sharing; (5) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls; (6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and (7) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Does My Company Need to Perform a Risk Assessment?

The regulation provides a one (1) year transition period for covered entities to perform a risk assessment, which should address technological developments, evolving threats, and the particular risks related to the entity's business operations, Nonpublic Information, and information systems and be performed whenever there is a material change to any of the aspects addressed by the assessment.[7] However, the regulation also provides that the cybersecurity program, cybersecurity policy, and access controls be based on the entity's risk assessment. Therefore, it is advisable for covered entities to perform at least a targeted risk assessment sufficient to inform the development of the entity's cybersecurity program, policy, and access control under the regulation. The risk assessment should be documented and carried out in accordance with written policies and procedures.

Looking Ahead: The First Certification and Second Transition Period Requirements

The deadline for covered entities to submit their first compliance certification is February 15, 2018. Shortly thereafter, on March 1, 2018, the second transition period will come to a close by which time covered entities must have implemented annual CISO reporting, penetration and vulnerability testing, a risk assessment, multi-factor authentication, and cybersecurity awareness training. These deadlines are fast-approaching, and covered entities may benefit from a gap analysis to determine the amount of work necessary to comply with the new regulations.

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 500.01 (c).
[3] 23 NYCRR 500 Appendix B.
[4] 23 NYCRR 500.19 provides a list of exemption qualifications, including covered 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."
[5] "Cybersecurity Event means 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." 23 NYCRR 500.01 (d).

[6] "Nonpublic Information shall mean all electronic information that is not Publicly Available Information and is: (1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual." 23 NYCRR 500.01(g).

[7] *See* 23 NYCRR 500.09. Note that all covered entities, including those that qualify for the limited exemption, are required to perform a risk assessment.