Akin Gump
STRAUSS HAUER & FELD LLP

Cybersecurity, Privacy & Data Protection Alert

January 19, 2017

Key Points

- A lawyer's role in cybersecurity is critical for Covered Entities. The New York Department of Financial Services recently revised cybersecurity regulations, which will require Covered Entities to implement a number of data security measures by March 1, 2017 and certify compliance as early as February 15, 2018.
- Key requirements of the revised regulations include: (i) incident response, (ii) breach notification, (iii) vendor management and (iv) compliance policies.
- Lawyers – whether in-house or external – must ensure that their multidisciplinary team has complied with standards imposed by regulators and ensure that the privilege is structured to maximize its protection in breach and compliance scenarios.

NYDFS: A Lawyer's Responsibility

New York Financial Regulator to Enforce First-of-Its-Kind Cybersecurity Regulations in Coming Weeks

On December 28, 2016, the New York Department of Financial Services (NYDFS) issued revised cybersecurity regulations that, as of March 1, 2017, will require Covered Entities—which broadly 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"—to implement a number of data security measures and certify compliance as early as February 15, 2018. The revised regulations were issued following an initial draft released on September 13, 2016 (Akin Gump blog post here), and a comment period during which more than 150 public comments regarding the initial regulations released on September 13, 2016, were filed.

Because the final NYDFS regulations will likely largely reflect the current draft of the regulations, companies subject to these regulations should immediately begin to tackle compliance requirements. By now, in-house counsel understand that cybersecurity is both a legal and a technical issue, where lawyers are a necessary and integral part of mitigating cybersecurity attacks and ensuring that reasonable security controls have met regulatory standards. Not only should lawyers ensure that their information security/technology departments are compliant with emerging regulations, but our lawyers consistently take the lead with respect to the following issues discussed more fully below: (1) incident response, (2) breach notification, (3) vendor management and (4) compliance.

Incident Response

Among other things, the regulations require each Covered Entity to "establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations." The NYDFS added the materiality threshold as part of its revisions to the rules, which should have a significant limiting effect, given the broad definition of a Cybersecurity Event: "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."

The regulations also require the incident response plan to address areas including the internal processes for responding to a Cybersecurity Event, goals of the plan, external and internal communications and information-sharing, and the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Since the regulation requires Covered Entities to regularly train all personnel, we assist daily with tailored scenario-planning and running tabletop exercises for all types of employees in connection with their cybersecurity awareness training.

Breach Notification

The NYDFS's original proposal required notification to DFS of a Cybersecurity Event within 72 hours and had encompassed "actual or potential authorized tampering with, or access to, or use of, Nonpublic Information." Following comments claiming that this was unduly burdensome and would result in over reporting of immaterial incidents, the revised regulations now set forth a materiality standard for reporting within 72 hours of a determination that the Event either (1) requires notice to any government body, self-regulatory agency or any other supervisory body; or (2) has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity.

One of our most important roles as lead breach counsel is determining whether the legal requirement to notify has been triggered and how other circumstances influence this decision-making process. The revised regulation still has a relatively broad notification trigger involving a "reasonable likelihood of materially harming any material part of the operations," and sound judgment is required to navigate the countless factors that impact notification considerations.

Vendor Management

Based on its Risk Assessment, each Covered Entity is required to implement written policies and procedures designed to ensure the security of information accessible to, or held by, "Third-Party Service Providers" (namely, a nonaffiliate that maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity). The policies and procedures should address the identification and risk assessment of Third-Party Service Providers, Third-Party Service Providers' minimum cybersecurity practices, due diligence processes and periodic assessment.

Our lawyers consistently help with development of third-party management programs and contract management, conducting diligence on, and negotiating, provisions that provide better oversight and control over Third-Party Service Providers relating to, among other things, access controls and encryption, representations and warranties concerning those policies and procedures, and notice of Cybersecurity Events.

Compliance Policies

The revisions establish a risk-based approach to cybersecurity policies, tying many of the requirements to the results of the Covered Entity's Risk Assessment, which must be conducted at least annually to "inform the design of the cybersecurity program" that is "updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations."

The rules require a Covered Entity to designate an individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy. This individual is referred to as a "CISO" (or Chief Information Security Officer) in the rules, although the CISO may be employed by an affiliate or Third-Party Service Provider. The CISO must submit written reports to the board of directors on an annual basis.

***

The role of the lawyer does not end there. Legal and compliance officers for Covered Entities should ensure that their information security/technology departments are aware that these standards exist and are implementing appropriate technical measures, and to whom and when they apply. For instance, the NYDFS regulations emphasize the importance of the following:

Data Retention

Each Covered Entity must include policies and procedures for the periodic disposal of nonpublic information that is no longer necessary for business operations or for other legitimate business purposes. The NYDFS previously exempted disposal where such information is otherwise required to be retained by law or regulation, and added to the revised version that disposal is not required where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Encryption and Multifactor Authentication

The NYDFS's original proposal broadly required multifactor authentication for virtually all network access and encryption for nearly all data. The revisions relax these requirements by requiring multifactor authentication for only individuals accessing internal networks from an external network when the CISO has not approved "reasonably equivalent or more secure access controls." Otherwise, only "effective controls" are required, which may include multifactor authentication or risk-based authentication. Further, where encryption is "infeasible," "effective alternative compensating controls reviewed and approved" by the CISO may be used.

Application and Exemptions

The NYDFS added a number of exemptions to the proposed regulations. In addition to exempting Covered Entities with less than $5 million in gross annual revenue in each of the last three fiscal years, several other Covered Entities are exempt: (1) fewer than 10 employees; (2) less than $10 million in year-end total assets; (3) employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity and is covered by the cybersecurity program of the Covered Entity; and (4) a Covered Entity that does not operate, maintain, utilize or control any Information Systems, and that does not control, own, access, generate, receive or possess Nonpublic Information.

Timeline

Covered Entities will have 180 days to comply with the requirements. However, the rules allow for extended implementation of some requirements, including the following:

Requirement	Deadline
CISO report	one year
Penetration testing	one year
Vulnerability assessments	one year
Risk assessments	one year
Multifactor authentication	one year
Updated cybersecurity awareness training	one year
Audit trail requirements	18 months
Application security	18 months
Data retention	18 months
Monitoring unauthorized access	18 months
Encryption	18 months
Policies and procedures for handling Third-Party Service Providers	two years*

*Although significant time is allowed for compliance with the Third-Party Service Provider provisions as compared to other requirements, we would recommend taking steps to implement this requirement sooner, given the high risk of third-party vendors, as well as the amount of time it takes to develop tailored written policies, conduct appropriate diligence efforts and negotiate protective contract language.

A lawyer's role in cybersecurity is critical for Covered Entities. In addition to taking the lead investigative role on data breach investigations and follow-on litigation, lawyers must ensure that their multidisciplinary team has complied with standards imposed by regulators and ensure that the privilege is structured to maximize its protection in breach and compliance scenarios.

Contact Information

If you have any questions regarding this alert, please contact:

Jo-Ellyn Sakowitz Klein
jsklein@akingump.com
+1 202.887.4220
Washington, D.C.

Natasha G. Kohne
nkohne@akingump.com
+971 2.406.8520 | Abu Dhabi
+1 415.765.9500 | San Francisco

Michelle A. Reed
mreed@akingump.com
+1 214.969.2713
Dallas

David S. Turetsky
dturetsky@akingump.com
+1 202.8874074
Washington, D.C.

Crystal Roberts
cgroberts@akingump.com
+1 415.765.9560
San Francisco