WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

New York Department of Financial Services Issues Amended Cybersecurity Regulations Affecting Financial Institutions, Insurers and Other Covered Entities

January 11, 2017

AUTHORS

Elizabeth P. Gray | David S. Katz | Leah Campbell | Marc J. Lederer | Philip F. DiSanto | Katherine Doty Hanniford

The New York Department of Financial Services ("DFS") proposed revised cybersecurity rules ("Cyber Rules") on December 28, 2016, following an active 45-day public notice-and-comment period.[1] In response to public comment, the DFS amended the Cyber Rules draft of September 2016 largely to make the Cyber Rules more risk-based. However, when promulgated, the revised Cyber Rules impose significant new regulatory burdens on companies supervised by the DFS ("Covered Entities").

"Covered Entities" are those entities supervised by the DFS that are doing business in New York and "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" of New York, such as banks and insurance companies. Cyber Rules § 500.01(c). Covered Entities may require additional investments in technology and expertise to comply with the Cyber Rules, which will be finalized in late January 2017 following a 30-day notice and public comment period.

[1] Cybersecurity Requirements for Financial Services Companies, available here (proposed Dec. 28, 2016) (to be codified at 23 NYCRR § 500). Our analysis of the DFS's earlier proposed Cyber Rules can be found in our November 3, 2016 Client Memo.

The Cyber Rules will become effective on March 1, 2017, and Covered Entities will be required to submit annual certificates of compliance to the DFS beginning February 15, 2018.

The most significant provisions of the Cyber Rules, and important changes from the Cyber Rules as initially proposed, are explained below.

Organizational & Compliance Requirements

All Covered Entities must **implement and maintain an internal cybersecurity program** to protect the "confidentiality, integrity and availability of the Covered Entity's Information Systems."[2] *Id.* § 500.02. The cybersecurity program must:

i. identify internal and external risks to Nonpublic Information ("NPI");

ii. use defensive infrastructure, policies, and procedures, to protect Information Systems;

iii. detect Cybersecurity Events[3];

iv. respond to, mitigate the effects of, and recover from Cybersecurity Events; and

v. fulfill all reporting obligations.

Id. § 500.02(b).

The cybersecurity program must be reviewed at least annually by either the board of directors or a Senior Officer of the Covered Entity (if no board of directors exists). *Id.* § 500.03(b).

All Covered Entities must also implement **written policies and procedures concerning risk assessment and conduct risk assessments** of the Covered Entity's Information Systems periodically, and must implement a **written incident response plan** to respond to and recover from any "Cybersecurity Event" that affects the Covered Entity's Information Systems or business. *Id.* § 500.09 & 500.16, respectively. Section 500.16(b) provides the minimum requirements for such a plan.

---

[2] *"Information System* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems." *Id.* § 500.01(e).

[3] *"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." *Id.* § 500.01(d).

The revised Cyber Rules provide more flexibility to Covered Entities in crafting their cybersecurity policies than as initially proposed. Instead of requiring a cybersecurity policy to address each enumerated area in the Cyber Rules, the DFS is allowing a Covered Entity to tailor its cybersecurity policy based upon its own risk assessment and operations. The revised Cyber Rules also permit a Covered Entity to adopt the cybersecurity program of an Affiliate,[4] provided such a program covers the Covered Entity's Information Systems and Nonpublic Information and meets the requirements of the revised Cyber Rules. DFS significantly narrowed the definition of "Nonpublic Information" to common combinations of personal identifiers that more closely align with similar definitions in many state data breach notification laws.

All Covered Entities must implement **written policies and procedures concerning Third-Party Service Providers**. *Id.* § 500.11. In response to criticism during the public comment period, the DFS made several significant revisions to the Cyber Rules with respect to Third-Party Service Providers,[5] including: (a) clarifications that the requirements of this section should be linked to the specific Covered Entity's Risk Assessment; (b) clarifications that Covered Entities are not obligated to audit Third-Party Service Providers; (c) the exclusion of Affiliates from the definition of "Third-Party Service Provider;" (d) among other changes to provisions in Third-Party Service Provider contracts, now requiring that Covered Entities maintain "relevant guidelines for due diligence and/or contractual protections relating to Third-Party Service Providers" instead of "preferred provisions to be included in contracts with Third-Party Service Providers;" and (e) adding an exemption for an employee, agent, or affiliate of a Covered Entity, that is itself a Covered Entity, to the extent that such employee, agent or affiliate is covered by the cybersecurity program of the Covered Entity. *Id.*

The revised Cyber Rules clarify that Covered Entities must designate a qualified individual to oversee and implement the Covered Entity's cybersecurity program and enforce its cybersecurity policy, serving as Chief Information Security Officer ("CISO") or comparable position. The Covered Entity may designate a Third-Party Service Provider or an Affiliate to fulfill these responsibilities in lieu of in-house personnel, provided that such a Third-Party Service Provider or Affiliate be overseen by a senior member of the Covered Entity's personnel and maintain a cybersecurity program that complies with the regulations. *Id.* § 500.04(a). All Covered Entities must **employ sufficient personnel** to fulfill the core functions required by the regulations and implement the written cybersecurity program and cybersecurity policy. *Id.* § 500.10(a). The Covered Entity must ensure that all authorized users of its Information Systems are **trained sufficiently** and must **monitor the activities of authorized users**. *Id.* § 500.14.

---

4 "*Affiliate* means any Person that controls, is controlled by or is under common control with another Person." The Cyber Rules consider the term "control" to mean "the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of stock of such Person or otherwise." *Id.* § 500.01(a).

5 "*Third-Party Service Provider(s)* means a Person that (i) is not an Affiliate of the Covered Entity, (ii) provides services to the Covered Entity, and (iii) maintains, processes or otherwise is permitted access to Nonpublic Information through its provision of services to the Covered Entity." *Id.* § 500.01(n).

Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities must conduct periodic **penetration testing** of the Covered Entity's Information Systems and bi-annual **vulnerability assessments**. *Id.* § 500.05.

Reporting Requirements

All Covered Entities must "**notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred**." *Id.* § 500.17(a). The revised Cyber Rules provide new flexibility by allowing a Covered Entity to report a Cybersecurity Event to the DFS only after a determination by the Covered Entity that a Cybersecurity Event as follows has occurred: "(1) Cybersecurity Events of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; and (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." *Id*. Nevertheless, the Cyber Rules still require that entities provide notice to the DFS of such triggering events within 72 hours of the Covered Entity's determination.

All Covered Entities must **document all areas that require material improvement, updating or redesign**, as well as efforts to remediate or address those areas, and make such documentation available for inspection to the Superintendent. *Id.* § 500.17(b).

The CISO or comparable person shall **provide an annual report to the board of directors**, a comparable governing body, or a Senior Officer if no such governing body exists. The report should address the state of the Covered Entity's Information Systems, the cybersecurity program and cybersecurity policy, current cyber risks to the Covered Entity, and a summary of all Cybersecurity Events during the time period since the last report. *Id.* § 500.04(b).

Technological Requirements

All Covered Entities must **limit access privileges** to Information Systems that allow access to NPI and must periodically review those privileges. *Id.* § 500.07. The revised Cyber Rules eliminate the requirement that Covered Entities use multi-factor authentication for certain privileged access to information systems and NPI, allowing Covered Entities to instead use risk-based authentication based upon their own risk assessments. In addition, a Covered Entity may forgo the use of multi-factor authentication for an individual accessing the Covered Entity's internal networks from an external network, if the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

The DFS revised its Cyber Rules regarding encryption to provide more flexibility to Covered Entities. First, the revised Cyber Rules clarify that Covered Entities may determine whether encryption should be used based upon each entity's own risk assessment. Covered Entities may conclude from their risk assessments that effective alternative compensating controls should be utilized instead of encryption. While under the previous draft Cyber Rules, alternative compensating controls were allowed to be used only for a period of one year for NPI in transit or for five years for NPI at rest after the Cyber Rules became effective, the revised Cyber Rules remove all such time restrictions. Additionally, the

revised Cyber Rules narrow the encryption requirement from encrypting "in transit" by replacing it with encrypting "in transit over external networks." Finally, the Cyber Rules were revised to require the CISO to review at least annually the feasibility of encryption and the effectiveness of alternative compensating controls.

Recordkeeping Requirements

All Covered Entities shall securely maintain **audit trail systems** that "(1) are designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Covered Entity; and (2) include audit trails designed to detect and respond to Cybersecurity Events that have **a reasonable likelihood of materially harming** any material part of the normal operations of the Covered Entity." *Id.* § 500.06(a) (emphasis added). The revised Cyber Rules provide new flexibility with respect to audit trail requirements. Instead of six enumerated categories for tracking and maintaining data, there are now three, and are only required "to the extent applicable and based on [the Covered Entity's] Risk Assessment." *Id.* This audit trail must be maintained for a minimum of five years. *Id.* § 500.06(b). The Cyber Rules also provide that Covered Entities must **implement policies and procedures for the secure disposal of NPI on a periodic basis**, where the NPI "is no longer necessary for business operations or for other legitimate business purposes of the Covered Entity," subject to certain exceptions. *Id.* § 500.13.

The revised Cyber Rules add a new confidentiality protection by specifying that information provided by a Covered Entity pursuant to the revised Cyber Rules is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law. *Id.* § 500.18.

The Department did not provide additional flexibility with respect to all problem areas highlighted by the public comments. For example, the defined terms "Cybersecurity Event," "Information System," and "Publicly Available Information" have not been narrowed, despite commentator concerns. And other provisions, though made slightly more flexible in the revised Cyber Rules, still impose new and onerous obligations on Covered Entities.

Covered Entities should familiarize themselves with these requirements prior to the March 1, 2017 effective date of the revised Cyber Rules. While additional changes may be made to the Cyber Rules during the current 30-day notice-and-comment period, familiarity with these basic requirements and expectations for specific industries will ease progress towards full compliance.

If you have any questions regarding this memorandum, please contact Elizabeth P. Gray (202-303-1207, egray@willkie.com), David S. Katz (202-303-1149, dkatz@willkie.com), Leah Campbell (212-728-8217, lcampbell@willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com), Philip F. DiSanto (212-728-8534, pdisanto@willkie.com), Katherine Doty Hanniford (202-303-1157, khanniford@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

January 11, 2017