SULLIVAN & CROMWELL LLP

January 3, 2017

DFS Issues Updated Proposed Cybersecurity Regulations

Responding to Industry Concerns, DFS Proposes More Flexible, Risk-Based Approach to Cybersecurity and Delays Implementation of Proposed Regulations

SUMMARY

On December 28, 2016, following a 45-day notice and public comment period, the New York Department of Financial Services (the "DFS") issued updated proposed cybersecurity regulations (the "Updated Proposed Regulations") applicable to banks, insurance companies, and other financial services institutions regulated by the DFS ("Regulated Institutions"). Intended to address concerns voiced by Regulated Institutions and trade associations with respect to the version originally proposed for comment in September 2016 (the "Original Proposed Regulations"), the Updated Proposed Regulations appear more flexible and more closely tied to each Regulated Institution's particular cybersecurity risk assessment. Moreover, the DFS has delayed the proposed regulations' implementation and has introduced transitional periods to permit Regulated Institutions additional time to come into compliance with certain requirements. Comments on the Updated Proposed Regulations are due January 27, 2017.

BACKGROUND

On September 13, 2016, the DFS issued the Original Proposed Regulations which, among other things, required Regulated Institutions to establish and maintain a cybersecurity program, implement and maintain cybersecurity policies and procedures, appoint a Chief Information Security Officer ("CISO"), and submit an annual certification of compliance with the regulations to the DFS.

Although the Original Proposed Regulations incorporated many industry practices, they were viewed as relatively prescriptive in approach and, in the opinion of many industry participants, did not sufficiently

account for Regulated Institutions' differing cyber-risk profiles. The Original Proposed Regulations thus would have constituted a departure from the more flexible assessment guidance issued by federal regulators.[1]

In response to the Original Proposed Regulations, the DFS received over 150 comments from individuals and entities, including Regulated Institutions and trade associations, as well as third-party service providers, including cybersecurity service providers.[2] Among other changes, several commentators proposed eliminating prescriptive minimum standards and delaying implementation of the regulations.

SUMMARY OF THE UPDATED PROPOSED REGULATIONS

Although the Updated Proposed Regulations represent a meaningful shift towards a more flexible, risk-based approach to cybersecurity, they nonetheless continue to prescribe a range of minimum cybersecurity requirements. The main changes from the Original Proposed Regulations are outlined below.

- **Risk Assessments.** The Updated Proposed Regulations no longer require annual risk assessments. Instead, they call for Regulated Institutions to conduct "periodic" risk assessments and update such risk assessments as reasonably necessary to address changes to the Regulated Institutions' information systems, nonpublic information, and business operations. The Updated Proposed Regulations explicitly tie the design of the cybersecurity program and the development of cybersecurity policies and procedures to such risk assessments. The DFS has, however, cautioned that risk assessments are not intended to permit Regulated Institutions to engage in a cost-benefit analysis of acceptable losses when faced with cybersecurity risks.[3]
- **Easing of Some Program and Policy Requirements.** The Updated Proposed Regulations relax a number of cybersecurity measures required to be included in Regulated Institutions' cybersecurity programs and policies. The Updated Proposed Regulations also adopt a more flexible approach to certain measures, requiring only that such measures be developed and adopted in accordance with Regulated Institutions' risk assessments. The modified measures include:
  - ***Data Retention and Destruction.*** The Original Proposed Regulations required Regulated Institutions to destroy certain nonpublic information that was no longer necessary to the provision of products or services for which the information was provided. The Updated Proposed Regulations allow Regulated Institutions to maintain nonpublic information if such information continues to be necessary for business operations or for other legitimate business purposes. In addition, Regulated Institutions are not required to dispose of nonpublic information if such disposal is not reasonably feasible due to the manner in which the information is maintained.[4]
  - ***Monitoring and Testing.*** The Original Proposed Regulations required all Regulated Institutions to conduct annual penetration testing and quarterly vulnerability assessments. The Updated Proposed Regulations instead require Regulated Institutions to develop monitoring and testing processes in accordance with their risk assessment. Such monitoring and testing must include either effective continuous monitoring or risk-based annual penetration testing and biannual vulnerability assessments.
  - ***Access Privileges.*** Departing from the proposed requirement that access to nonpublic information be limited to individuals who require such access to perform their responsibilities, the Updated Proposed Regulations instead require Regulated Institutions to design access limits based on their risk assessment.

- ***Multifactor Authentication.*** Instead of requiring multifactor authentication and risk-based authentication in a range of specified circumstances, the Updated Proposed Regulations generally permit Regulated Institutions to select appropriate controls, which may include multifactor or risk-based authentication, based on their risk assessment. The Updated Proposed Regulations do, however, continue to require the use of multifactor authentication for access to a Regulated Institution's internal systems or data from an external network, unless the Regulated Institution's CISO has approved in writing the use of reasonably equivalent or more secure access controls.

- ***Encryption.*** The Updated Proposed Regulations continue to call for the encryption of data in transit and at rest; however, the original grace periods for the implementation of such encryption (one year for data in transit and five years for data at rest) have been replaced by an indefinite permission to use compensating controls approved by the CISO so long as the Regulated Institution determines encryption is infeasible. The CISO must review the feasibility of encryption and effectiveness of the compensating controls at least annually.

- **Audit Trail.** The audit trail requirements in the Original Proposed Regulations have been significantly reduced and relaxed. The Updated Proposed Regulations require that, to the extent applicable and based on the Regulated Institution's risk assessment, each Regulated Institution securely maintain systems that are designed to reconstruct material financial transactions and that include audit trails designed to detect and respond to cybersecurity events that have a reasonable likelihood of materially harming any part of the normal operations of the Regulated Institution. The audit trail record-keeping requirements have also been reduced from six to five years.

- **Third-Party Service Providers.** As was the case with the Original Proposed Regulations, the Updated Proposed Regulations require Regulated Institutions to implement written policies and procedures designed to ensure the security of information systems and nonpublic information accessible to or held by third-party service providers. The Original Proposed Regulations required such policies and procedures to establish preferred provisions to be included in contracts with third-party service providers, including provisions addressing a range of listed areas. The Updated Proposed Regulations instead require that the policies and procedures include "relevant guidelines for due diligence and/or contractual protections" relating to third-party service providers. The areas that these guidelines must address have also been narrowed: the policies and procedures need not address the provision of identity theft protection products by third-party service providers after a breach nor the right of Regulated Institutions to perform cybersecurity audits of third-party service providers.

- **Nonpublic Information.** Some commentators expressed concern about the breadth and clarity of the definition of "nonpublic information" in the Original Proposed Regulations and suggested that the definition should more closely track the language of other cybersecurity standards. The DFS responded to these comments by revising the definition in the Updated Proposed Regulations. The revised definition focuses to a greater extent on the nature of the information in question (*e.g.*, health information, Social Security numbers) rather than the circumstances under which the information was obtained (*e.g.*, in connection with the provision of financial products or services to an individual). In addition, "information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual" will be considered nonpublic information only when combined with one of several more sensitive data elements listed in the Updated Proposed Regulations (*e.g.*, Social Security number, credit or debit card number, biometric records).

- **Notice to DFS of Cybersecurity Events.** Pursuant to the Updated Proposed Regulations, Regulated Institutions must notify the DFS of a cybersecurity event within 72 hours of determining that a cybersecurity event meets the notice criteria, rather than the originally proposed 72 hours of the event itself (a standard that many commentators considered infeasible). Moreover, the harm-based trigger for notice has been narrowed. The Original Proposed Regulations required notice of any Cybersecurity Event that "has a reasonable likelihood of materially affecting the normal operation of the [Regulated Institution] or that affects Nonpublic Information,"

including "any Cybersecurity Event involving the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information." The revised regulations require notice if there is "a reasonable likelihood of materially harming any material part of the normal operation(s)" of the Regulated Institution.

- **Affiliates.** Regulated Institutions may now comply with several requirements of the Updated Proposed Regulations through Affiliates.[5] Regulated Institutions may:
  - Adopt a cybersecurity program maintained by an Affiliate, so long as such program satisfies the requirements of the Updated Proposed Regulations and covers the Regulated Institution's information systems and nonpublic information.
  - Designate a CISO employed by an Affiliate, provided the Regulated Institution retains responsibility for compliance with the Updated Proposed Regulations.
  - Utilize qualified cybersecurity personnel of an Affiliate.
- **Chief Information Security Officer.** The Original Proposed Regulations were interpreted by some to require the appointment of a CISO whose exclusive function is overseeing and implementing the cybersecurity program and enforcing cybersecurity policies. The Updated Proposed Regulations clarify that, although Regulated Institutions must designate a qualified individual to perform the functions of a CISO, that individual need not have a specific title and can perform other functions as well. Moreover, the Updated Proposed Regulations require that the CISO report in writing at least annually to the Board of Directors or an equivalent governing body, or to a senior officer. The Original Proposed Regulations had called for biannual reports.
- **Confidentiality.** The Updated Proposed Regulations state that information provided by a Regulated Institution pursuant to the proposed regulations "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." This addition comes in response to concerns expressed by some industry participants regarding the confidentiality of information that must be provided to the DFS under the proposed regulations. In addition to requiring notices of cybersecurity events, the Updated Proposed Regulations also provide for increased transparency on the part of Regulated Institutions. Specifically, documentation and information relevant to Regulated Institutions' cybersecurity program must be made available to the DFS upon request, and records, schedules, and data supporting the annual certificate of compliance must be made available for examination.
- **Exemptions.** The Updated Proposed Regulations expand the categories of entities that may claim an exemption from some or all of the regulations' requirements. Regulated Institutions claiming an exemption must file a notice of exemption with the DFS. The following categories of entities are now eligible for certain exemptions:
  - Regulated Institutions with (a) fewer than 10 employees; (b) less than $5,000,000 in gross annual revenues in each of the last three fiscal years; or (c) less than $10,000,000 in year-end total assets, calculated in accordance with GAAP, including assets of Affiliates, are exempt from a number of the regulations' requirements, including appointment of a CISO, monitoring and testing of information systems, use of encryption or compensating controls, and maintenance of a written incident response plan.
  - Employees, agents, representatives or designees of a Regulated Institution, who are themselves a Regulated Institution, are exempt from the proposed regulations entirely and need not develop their own cybersecurity program if such persons are covered by the cybersecurity program of the Regulated Institution.
  - Regulated Institutions that do not directly or indirectly operate, maintain, utilize, or control any information systems and that do not, and are not required to, directly or indirectly control, own, access, generate, receive or possess nonpublic information will only be subject to the requirements relating to risk assessments, implementation of written third-party service provider policies, disposal of nonpublic information, and notices to the DFS.

- **Effective Date.** The effective date of the Updated Proposed Regulations has been postponed from January 1, 2017 to March 1, 2017.
- **Transitional Period.** In a departure from the Original Proposed Regulations, the Updated Proposed Regulations introduce the following transitional periods for Regulated Entities to come into compliance:
  - One year from the effective date for the requirements relating to reporting by the CISO to the Board of Directors, equivalent body or senior officer; monitoring and testing of information systems; carrying out of risk assessments; use of controls against unauthorized access such as multifactor authentication and risk-based authentication; and provision of regular cybersecurity awareness training.
  - Eighteen months from the effective date for the requirements relating to maintenance of an audit trail; security of in-house and externally developed applications; limits on data retention; the implementation of risk-based policies, procedures and controls to monitor activity of authorized users and to detect unauthorized users; and use of encryption or compensating controls.
  - Two years from the effective date for the requirements relating to third-party service provider policies.

The Updated Proposed Regulations will be finalized following a second notice and public comment period of 30 days. The DFS will focus its final review on any *new* comments not previously raised in the original comment process.

Regulated Institutions should review the Proposed Regulations and evaluate their own cybersecurity policies, procedures, and programs against the Proposed Regulations' requirements. Some Regulated Institutions may also wish to participate in the 30-day notice and public comment period, whether directly or through industry associations.

* * *

ENDNOTES

1 *See, e.g.*, Federal Financial Institutions Examination Council, Cybersecurity Assessment Tool, *available at* https://www.ffiec.gov/cyberassessmenttool.htm.

2 New York Department of Financial Services, Assessment of Public Comments for New Part 500 to 23 NYCRR, *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500apc.pdf.

3 New York Department of Financial Services, Assessment of Public Comments for New Part 500 to 23 NYCRR, *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500apc.pdf.

4 For example, some commentators noted that "data stored on magnetic tapes and commingled data on servers present significant feasibility challenges with respect to any requirement for targeted data destruction." Comment Letter from the Securities Industry and Financial Markets Association, American Bankers Association, Financial Services Roundtable, Financial Services Sector Coordinating Council, Mortgage Bankers Association, American Financial Services Association, American Land Title Association and New York Mortgage Bankers Association, dated November 14, 2016, *available at* http://www.aba.com/Advocacy/commentletters/Documents/SIFMA-NY-DFS-Proposed-Cyber-Requirements.pdf.

5 "Affiliate" is defined as "any Person that controls, is controlled by or is under common control with another Person." For the purpose of this definition, "control" means "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."

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, three offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future related publications from Michael B. Soleta (+1-212-558-3974; soletam@sullcrom.com) in our New York office.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Nader A. Mousavi	+1-212-558-1624	mousavin@sullcrom.com
William D. Torchiana	+1-212-558-4056	torchianaw@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Eric J. Kadel, Jr.	+1-202-956-7640	kadelej@sullcrom.com
Brent J. McIntosh	+1-202-956-6930	mcintoshb@sullcrom.com
Stephen H. Meyer	+1-202-956-7605	meyerst@sullcrom.com
Jennifer L. Sutton	+1-202-956-7060	suttonj@sullcrom.com
Samuel R. Woodall III	+1-202-956-7584	woodalls@sullcrom.com
Palo Alto		
Scott D. Miller	+1-650-461-5620	millersc@sullcrom.com
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Paris		
William D. Torchiana	+33-1-7304-5890	torchianaw@sullcrom.com