PAUL HASTINGS

STAY CURRENT

February 2017

Follow @Paul_Hastings

New York's New Cybersecurity Rule for Financial Institutions & How It May Affect You

By Behnam Dayanim & Quinn Dang

New York's top banking regulator, the New York Department of Financial Services ("NYDFS"), recently issued a revised rule, effective March 1, 2017, that requires banks, insurance companies and other financial institutions regulated by NYDFS to establish and maintain a comprehensive cybersecurity program to respond to the growing threat of cyber-attacks.

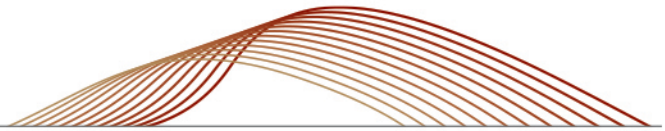
The revised rule responds to some of the criticisms that have poured in during the comment period following the issuance of the original rule in September. Although the revised rule preserves the core cybersecurity framework in the original rule, including the requirement to appoint a Chief Information Security Officer (CISO), the revision in general introduces more flexibility by permitting institutions to tailor their cybersecurity policies and programs to the size of the company and the specific cyber risks they face. Additionally, it now requires that the cybersecurity program be designed to "protect" (vs. "ensure") the confidentiality, integrity and availability of the entity's information systems.

Key Differences:

Other key differences include:

- **Risk-Assessment.**[1] The revision incorporates the concept of risk assessment as a key component throughout various sections of the rule to allow an institution to adjust its cybersecurity program according to the specific risks it faces. For example, the revision specifically requires the cybersecurity program to be based on a covered entity's risk assessment.[2] The revision requires that entities update such risk assessments as "reasonably" necessary to address changes to the information systems and to respond to technological developments and evolving threats and particular risks to the entity's business operations related to cybersecurity. Risk assessments need only be conducted "periodically" (rather than annually as required by the original draft).

- **Definition of nonpublic.**[3] The definition of "nonpublic information" has been narrowed to cover only information that is not publicly available and identifies an individual through any one or more of: (i) Social Security number, (ii) driver's license number, (iii) account number, credit or debit number, (iv) security code, access code or password or (v) biometric records; or any information from a health care provider that relates to the individual's health, provision of care or payment.



- **CISO**.[4] The rule expressly states that the CISO who is responsible for overseeing the cybersecurity program may be an affiliate or a third-party service provider. The company, even if it appoints a third-party provider, retains responsibility for compliance and must designate a senior member to direct and oversee the third-party provider. Additionally, the CISO must report to a board or equivalent.

- **Incident Response Plan**.[5] The revision still requires entities to have a written incident response plan to respond to a cybersecurity event, but now limits the scope of the requirement to events that "materially" affect the integrity of the entity's information systems, or any aspect of the business or operations.

- **Encryption**.[6] The revised rule does not specifically require encryption, but instead requires that a covered entity, based on its risk assessment, implement controls (such as encryption) to protect nonpublic information. To the extent that the entity determines that encryption is "infeasible," it may secure nonpublic information with "effective alternative compensating controls," as approved by the CISO. Entities have 18 months to comply with this requirement.

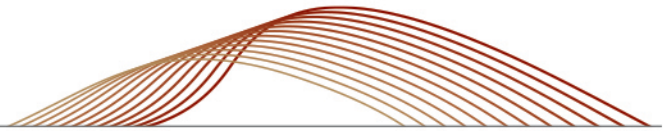
- **Monitoring and Penetration Testing**.[7] The revised rule requires entities **either** to monitor its cybersecurity program "continuously," **or** to conduct annual penetration testing and a bi-annual vulnerability assessment.

- **Multi-Factor Authentication**.[8] Based on its risk assessment, each institution must use effective controls, such as multi-factor authentication or risk-based authentication, to protect against unauthorized access. Multi-factor authentication is required for individuals accessing an entity's internal networks from an external network, unless the CISO has approved in writing of the use of reasonably equivalent or more secure access controls.

- **Breach Notice**.[9] One significant change to the proposed rule is the requirement that firms report breaches within 72 hours from when the breach was discovered. Previously, the rule's 72-hour clock started from the time of the actual breach. Moreover, entities do not have to report every cybersecurity incident because under the revision, only cybersecurity events that "have a reasonable likelihood of materially harming any material part of the normal operation(s)" or those where notice is required to be provided to any other government body trigger the reporting requirement. Existing New York law requires notice to the state attorney general when certain categories of personal information (defined similarly to "nonpublic information" under the proposed rule) are compromised.

- **Data Retention**.[10] The rule requires that a company have policies to dispose on a periodic basis of nonpublic information no longer necessary for the business operations or for other legitimate business purposes, except where targeted disposal is not reasonably feasible due to the manner in which the information is maintained. Entities have 18 months to comply with this requirement.[11]

- **Exemptions**.[12] Rather than create exemptions based on customer volume as originally proposed, the revised rule exempts from certain of the proposed rule's requirements entities with fewer than 10 employees, or less than $5 million in gross annual revenue in the last three fiscal years, or less than $10 million in year-end total assets. Entities claiming an exemption must notify NYDFS.



- **Deadline.**[13] The revision pushes the deadline back from January to March 2017, and creates new staggered implementation dates for certain provisions.

Take-aways:

The rule has far-reaching implications.

1. Covered Entities. First, the rule reaches not just banks and insurance companies, but also third-party service providers of these entities. The rule requires that such third parties that engage with a regulated entity also have a security policy in place. Third parties will also need to maintain minimum cybersecurity practices and will be subject to periodic assessments.

2. Comprehensive Cybersecurity Policies and Programs. Second, the rule is one of the first of its kind to require companies to adopt comprehensive cybersecurity policies and programs. As such, other states will certainly be watching as New York implements the rule, and similar proposals may emerge across the country. The rules may serve as a guidepost for legislators and regulators, and help to define what is "reasonable" for the purposes of enforcement actions on the state and federal levels.

The revised rule remains open for public comment but, as noted, will take effect on March 1. If you have any questions regarding the rule or compliance with the new requirements, please contact a member of our Privacy & Cybersecurity Practice.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

New York

James H. Koenig
1.212.318.6005
jimkoenig@paulhastings.com

San Francisco

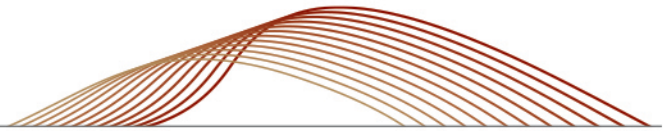
Thomas P. Brown
1.415.856.7248
tombrown@paulhastings.com

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
behnamdayanim@paulhastings.com

Sherrese M. Smith
1.202.551.1965
sherresesmith@paulhastings.com



[1] N.Y. Comp. Codes R. & Regs. tit. 23§§ 500.02, 500.09 (2016).

[2] § 500.03.

[3] § 500.01(g).

[4] §500.04.

[5] § 500.16.

[6] §500.15.

[7] §500.05.

[8] §500.12.

[9] §500.17.

[10] §500.13.

[11] §500.22(b)(2).

[12] §500.19.

[13] §500.21.