NEW YORK STATE
DEPARTMENT*of*
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Anthony J. Albanese
Acting Superintendent

FROM: Anthony J. Albanese, Acting Superintendent of Financial Services

TO: Financial and Banking Information Infrastructure Committee (FBIIC) Members:

Federal Reserve Board of Governors; Office of the Comptroller of the Currency (OCC); Commodities Futures Trading Commission (CFTC); U.S. Department of the Treasury; Securities and Exchange Commission (SEC); Federal Deposit Insurance Commission (FDIC); Federal Housing Finance Agency (FHFA); Consumer Financial Protection Bureau (CFPB); National Credit Union Administration (NCUA); Federal Reserve Bank of New York (FRBNY); Federal Reserve Bank of Chicago; National Association of Insurance Commissioners (NAIC); Conference of State Bank Supervisors (CSBS); American Council of State Savings Supervisors; Farm Credit Administration (FCA); National Association of State Credit Union Supervisors (NASCUS); North American Securities Administrators Association (NASAA); Securities Investor Protection Corporation (SIPC)

RE: Potential New NYDFS Cyber Security Regulation Requirements

DATE: November 9, 2015

We write today regarding potential new regulations from the New York State Department of Financial Services (NYDFS) aimed at increasing cyber security defenses within the financial sector. It is our hope that this letter will help spark additional dialogue, collaboration and, ultimately, regulatory convergence among our agencies on new, strong cyber security standards for financial institutions.

The New York State Department of Financial Services considers cyber security to be among the most critical issues facing the financial world today—and one that poses a particular challenge to regulatory agencies. As such, we have taken a number of steps in recent years to highlight and identify existing and emerging cyber security risks at banks and insurance companies.

In 2013, the Department conducted a survey of more than 150 of its regulated banking organizations about their cyber security programs, costs and future plans. The Department conducted a similar survey of 43 of its regulated insurers in 2013 and 2014. After reviewing and analyzing the responses, the Department published reports of its key findings in May 2014 and February 2015. The May 2014 report is available at http://www.dfs.ny.gov/about/press2014/

pr140505_ cyber_security.pdf, and the February 2015 report is available at http://www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf.

The findings from these initial surveys led to several additional actions. First, the Department has expanded its information technology ("IT") examination procedures to focus more attention on cyber security. As part of this revised examination process, the Department began conducting risk assessments of its financial institutions in late 2014 and early 2015 (the initial letters requesting information can be found at http://www.dfs.ny.gov/banking/bil-2014-10-10_cyber_security.pdf and http://www.dfs.ny.gov/about/press2015/pr150326-ltr.pdf) to gather information about industry-wide risks and vulnerabilities, as well as to help prioritize the scheduling of examinations.

Second, the cyber security reports highlighted the financial industry's reliance on third-party service providers for critical banking and insurance functions as a continuing challenge. The Department surveyed an additional sample of regulated banking organizations in October 2014 about the practices currently in place surrounding the management of their third-party service providers, and published an April 2015 update to its earlier report highlighting the most critical observations, which can be viewed at http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf. The Department has also surveyed a sample of its insurers about their third-party service providers as part of its risk assessments.

Several broad conclusions and concerns have emerged from these reports and the risk assessments (the latter of which are still ongoing), as well as from the dozens of discussions that the Department has held with its regulated entities, cyber security experts, and other stakeholders. First, although financial institutions have taken significant steps to bolster cyber security efforts in recent years, companies will continue to be challenged by the speed of technological change and the increasingly sophisticated nature of threats. Cyber security programs must remain dynamic to keep pace with this fast-changing landscape. Second, third-party service providers often have access to sensitive data and to a financial institution's information technology systems, providing a potential point of entry for hackers. A company may have the most sophisticated cyber security protections in the industry, but if its third party service providers have weak systems or controls, those protections will be ineffective. Finally, the scale and breadth of the most recent breaches and incidents demonstrate that cyber security is a global concern that affects every industry at all levels.

There is a demonstrated need for robust regulatory action in the cyber security space, and the Department is now considering a new cyber security regulation for financial institutions. The Department believes that it would be beneficial to coordinate its efforts with relevant state and federal agencies to develop a comprehensive cyber security framework that addresses the most critical issues, while still preserving the flexibility to address New York-specific concerns. To that end, this letter sets forth the key regulatory proposals that we are currently considering and we invite your feedback. The Department welcomes the opportunity to work with other regulators to develop a comprehensive approach to cyber security regulation in the weeks and months ahead.

* * *

We expect that potential regulations put forward by our Department would require covered entities to maintain a cyber security program designed to perform core cyber security functions and would set specific requirements in the following areas, among others:

Cyber Security Policies and Procedures

Covered entities would be required to implement and maintain written cyber security policies and procedures that address the following areas:

(1) information security;
(2) data governance and classification;
(3) access controls and identity management;
(4) business continuity and disaster recovery planning and resources;
(5) capacity and performance planning;
(6) systems operations and availability concerns;
(7) systems and network security;
(8) systems and application development and quality assurance;
(9) physical security and environmental controls;
(10) customer data privacy;
(11) vendor and third-party service provider management; and
(12) incident response, including by setting clearly defined roles and decision making authority.

Third-party Service Provider Management

Each covered entity would be required to implement and maintain policies and procedures to ensure the security of sensitive data or systems that are accessible to, or held by, third party service providers. The policies and procedures would be required to include internal requirements for minimum preferred terms to be included in contracts with third-party service providers, including provisions requiring:

(1) the use of multi-factor authentication to limit access to sensitive data and systems;
(2) the use of encryption to protect sensitive data in transit and at rest;
(3) notice to be provided in the event of a cyber security incident;
(4) the indemnification of the entity in the event of a cyber security incident that results in loss;
(5) the ability of the entity or its agents to perform cyber security audits of the third party vendor; and
(6) representations and warranties by the third party vendors concerning information security.

Multi-Factor Authentication

The Department believes that any regulation that establishes cyber security program requirements for covered entities should also address the use of multi-factor authentication as it applies to (i) customer access to web applications that captures or displays confidential information; (ii) privileged access to database servers that allow access to confidential information; and (iii) any access to internal systems or data from an external network. To this

end, covered entities would be required, among other things, to implement multi-factor authentication for all access to internal systems and data from an external network.

Chief Information Security Officer

Each covered entity would be required to designate a qualified employee to serve as its Chief Information Security Officer ("CISO") responsible for overseeing and implementing its cyber security program and enforcing its cyber security policy. The CISO would also be required to submit to the Department an annual report, reviewed by the entity's board, assessing the cyber security program and the cyber security risks to the entity.

Application Security

Each covered entity would be required to maintain and implement written procedures, guidelines, and standards reasonably designed to ensure the security of all applications utilized by the entity. The CISO would be required to review and update all such procedures, guidelines, and standards at least annually.

Cyber Security Personnel and Intelligence

Each covered entity would be required to employ personnel adequate to manage the entity's cyber security risks and perform the core cyber security functions of identify, protect, detect, respond and recover. The entity would also be required to provide mandatory training to cyber security personnel and require key cyber security personnel to stay abreast of changing cyber security threats and countermeasures. Entities would be able to use third parties in meeting such requirements.

Audit

Each covered entity would be required to conduct annual penetration testing and quarterly vulnerability assessments. Entities also would be required to maintain an audit trail system that:

(1) logs privileged user access to critical systems;
(2) protects log data stored as part of the audit trail from alteration or tampering;
(3) protects the integrity of hardware from alteration or tampering; and
(4) logs system events, including access and alterations made to audit trail systems.

Notice of Cyber Security Incidents

Each covered entity would be required to immediately notify the Department of any cyber security incident that has a reasonable likelihood of materially affecting the normal operation of the entity, including any cyber security incident:

(1) that triggers certain other notice provisions under New York Law;
(2) of which the entity's board is notified; or
(3) that involves the compromise of "nonpublic personal health information" and "private information" as defined under New York Law, payment card information or any biometric data.

* * *

While the proposals described above are the product of the Department's analysis and discussion in this area to date, they do not represent a complete list and may be subject to further revision as the Department continues to review and discuss these issues. Should you have any questions or wish to engage in a discussion about these proposals, please contact Maria Filipakis, Executive Deputy Superintendent of the Capital Markets Division, at (212) 709-1605. We look forward to working with you on these important issues.