NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

TO: All NYS-Chartered or Licensed Banking Institutions

FROM: Benjamin M. Lawsky

DATE: December 10, 2014

RE: New Cyber Security Examination Process

In an effort to promote greater cyber security across the financial services industry, the New York State Department of Financial Services (the "Department") plans to expand its information technology ("IT") examination procedures to focus more attention on cyber security. The Department encourages all institutions to view cyber security as an integral aspect of their overall risk management strategy, rather than solely as a subset of information technology. To that end, the Department has incorporated into the examination new questions and topics, which will be embodied in pre-examination "First Day Letters."

In particular, IT/cyber security examinations will now include, but not be limited to, the following topics:

- Corporate governance, including organization and reporting structure for cyber security related issues;
- Management of cyber security issues, including the interaction between information security and core business functions, written information security policies and procedures, and the periodic reevaluation of such policies and procedures in light of changing risks;
- Resources devoted to information security and overall risk management;
- The risks posed by shared infrastructure;
- Protections against intrusion including multi-factor or adaptive authentication and server and database configurations;
- Information security testing and monitoring, including penetration testing;
- Incident detection and response processes, including monitoring;
- Training of information security professionals as well as all other personnel;
- Management of third-party service providers;
- Integration of information security into business continuity and disaster recovery policies and procedures; and
- Cyber security insurance coverage and other third-party protections.

As is standard with both safety and soundness and targeted examinations, each institution may receive a tailored First Day Letter at the time that the institution is actually scheduled for examination.

In addition to the revised First Day Letter, the Department is updating its examination process, including the procedure for assessing and scheduling IT/cyber security examinations. Going forward, the Department will schedule IT/cyber security examinations following the comprehensive risk assessment of each institution. To aid in that assessment, the Department will be seeking, by separate request, responses to the following questions:

1. Provide the CV and job description of the current Chief Information Security Officer or the individual otherwise responsible for information security, describe that individual's information security training and experience, and identify all reporting lines for that individual, including all committees and managers. In addition, provide an organization chart for your institution's IT and information security functions.

2. Describe the extent to which your institution maintains information security policies and procedures designed to address the information security goals of confidentiality, integrity, and availability. Provide copies of all such information security policies.

3. Describe how data classification is integrated into information risk management policies and procedures.

4. Describe your institution's vulnerability management program as applicable to servers, endpoints, mobile devices, network devices, systems, and applications.

5. Describe the organization's patch management program including how updates, patches, and fixes are obtained and disseminated, whether processes are manual or automated, and how often they occur.

6. Describe identity and access management systems employed by the organization for both internal and external users, including all administrative, logical, and physical controls and whether such controls are preventive, detective, or corrective in nature.

7. Identify and describe the current use of multi-factor authentication for any systems or applications.

8. Describe your institution's due diligence process regarding information security practices that is used in vetting, selecting, and monitoring third-party service providers.

9. Describe all application development standards utilized by the organization, including the use of a secure software development life cycle, and the extent to which security and privacy requirements are assessed and incorporated into the initial phases of the application development process.

10. Provide a copy of, to the extent it exists in writing, or otherwise describe, the organization's incident response program, including how incidents are reported, escalated, and remediated.

11. Describe the extent to which information security is incorporated into the organization's BCP/DR plan, how and how often the BCP/DR is tested, and the results of the most recent test.

12. Describe any significant changes to the institution's IT portfolio over the last 24 months resulting from mergers, acquisitions, or the addition of new business lines.

Benjamin M. Lawsky
Superintendent of Financial Services