



NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Benjamin M. Lawsky
Superintendent

March 26, 2015

Dear Chief Executive Officer, General Counsel, and Chief Information Officer:

In an effort to promote greater cyber security across the financial services industry, the New York State Department of Financial Services (the “Department”) has expanded 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 intends to incorporate new questions and topics into the existing IT examination framework.

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.

The Department intends to schedule IT/cyber security examinations after conducting a comprehensive risk assessment of each institution. To aid in that assessment, the Department hereby requests a report pursuant to its authority under New York Insurance Law Sections 308

and 1504(a) in the form of the information requested below and completion of the Platform Data Sheet, attached hereto as Appendix A. If any part of your response requires your institution to access information in the possession of a parent or affiliate, please make every effort to do so pursuant to Section 1504(a)(2). Please note that an insurer must obtain such information from a subsidiary.

The report should:

1. Provide the curriculum vitae 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, networks, endpoints, mobile devices, network devices, systems, and applications;
5. Describe your institution'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 your institution 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 networks, systems, programs, or applications;
8. Describe all application development standards used by your institution, 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;
9. Provide a copy of, to the extent it exists in writing, or otherwise describe, your institution's incident response program, including how incidents are reported, escalated, and remediated;
10. Describe the extent to which information security is incorporated into your institution's business continuity and disaster recovery plan, the way in which that plan is tested, how often the plan is tested, and the results of the most recent test;

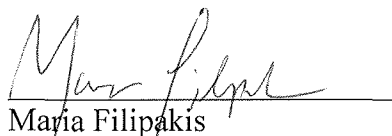
11. Describe any significant changes to your institution's IT portfolio over the last 24 months resulting from mergers, consolidations, acquisitions, or the addition of new business lines;
12. Describe your institution's due diligence process regarding information security practices that is used in vetting, selecting, and monitoring third-party service providers;
13. Provide a copy of any policies and procedures governing relationships with third-party service providers that address information security risks, including setting minimum information security practices or requiring representations and warranties concerning information security;
14. Describe any steps your institution has taken to adhere to the Framework for Improving Critical Infrastructure Cybersecurity issued by the National Institute of Standards and Technology ("NIST") on February 12, 2014 concerning third-party stakeholders;
15. Describe any protections that your institution uses to safeguard sensitive data that is sent to, received from, or accessible to third-party service providers, such as encryption or multi-factor authentication; and
16. List any and all protections against loss or damage incurred by your institution as a result of an information security failure by a third-party service provider, including any relevant insurance coverage.

Please submit your responses via the Department's secure portal application no later than April 27, 2015. Should you have any questions regarding this letter or the requested report, please do not hesitate to contact Mark Silver, Assistant Counsel, at mark.silver@dfs.ny.gov or (212) 709-3862.

Very truly yours,

Benjamin M. Lawsky
Superintendent of Financial Services

By:



Maria Filipakis
Executive Deputy Superintendent - Capital Markets Division
New York State Department of Financial Services
One State Street
New York, NY 10004-1511