NEW YORK STATE
DEPARTMENT of
FINANCIAL SERVICES

Andrew M. Cuomo
Governor

Benjamin M. Lawsky
Superintendent

October 21, 2014

To the Chief Executive, General Counsel and Chief Information Officer:

In light of the increasing number and sophistication of cyber attacks against financial services institutions, the New York State Department of Financial Services ("the Department") is currently reviewing how financial institutions manage third-party relationships with respect to cybersecurity. It is abundantly clear that, in many respects, a firm's level of cybersecurity is only as good as the cybersecurity of its vendors. As noted previously in our May 6, 2014 report on cybersecurity in the banking sector, the Department is concerned about the level of insight financial institutions have into the sufficiency of the cybersecurity controls of their third-party service providers. It is important that financial institutions are able to identify, monitor, and mitigate any cybersecurity risks posed by their third-party relationships, including but not limited to law firms and accounting firms.

The Department is therefore considering a requirement that financial institutions obtain representations and warranties from their third-party vendors with regard to the third parties' cyber security standards and policies. We therefore request a Special Report pursuant to New York State Banking Law 37(3) in the form of your response to the below set of questions. The Special Report is considered supervisory material covered by Section 36.10 of the New York State Banking law and is therefore afforded confidential treatment. Please furnish your responses by close of business on November 4, 2014.

1. Describe any due diligence processes used to evaluate the adequacy of information security practices of third-party service providers.

2. 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.

3. 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.

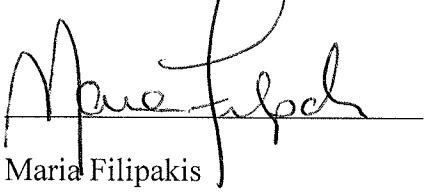
4. Describe any protections used to safeguard sensitive data that is sent to, received from, or accessible to third-party service providers, such as encryption or multi-factor authentication.

5. List any and all protections against loss incurred as a result of an information security failure by a third-party service provider, including any relevant insurance coverage.

Should you have any questions regarding the contents of this letter, please contact Colleen O'Brien, Senior Counsel, Capital Markets Division (Colleen.OBrien@dfs.ny.gov; 212-709-3817).

Sincerely,

Benjamin M. Lawsky
Superintendent of Financial Services



Maria Filipakis
Executive Deputy Superintendent of Capital Markets