



January 25, 2016

Via Electronic Mail (maria.filipakis@dfs.ny.gov)

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

Re: Letter to Financial and Banking Information Infrastructure Committee (FBIIC) Members:
Potential New NYDFS Cyber Security Regulation Requirements

Dear Ms. Filipakis:

The Securities Industry and Financial Markets Association (“SIFMA”)¹ submits this letter to the New York State Department of Financial Services (“NYDFS”) in connection with the letter that was sent to the members of the Financial and Banking Information Infrastructure Committee (FBIIC) on November 9, 2015.² SIFMA commends the NYDFS for initiating a dialog with the FBIIC to collaborate with the other financial regulatory agencies in the United States to drive regulatory convergence of cybersecurity standards. This is action we have been advocating since the release of our Principles for Effective Cybersecurity Regulatory Guidance³. That document provides regulators with SIFMA members' insight on productive ways to harmonize and create effective cybersecurity regulatory guidance. In addition, we appreciate the NYDFS providing the industry with the opportunity to submit early recommendations on the proposed set of potential regulations that would apply to certain ‘covered entities’ as presented in the letter.

Cybersecurity is a top priority for the financial industry to ensure the security of sensitive information and customer/client data, as well as efficient, reliable operations given the risks of cyber attack. Our members believe taking a risk-based approach enables a covered entity to develop and implement a cybersecurity program that effectively mitigates their respective technology and cyber risks. They should recognize that there is no one-size-fits-all approach to

¹ The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit <http://www.sifma.org>.

² Link to letter, http://www.dfs.ny.gov/about/letters/pr151109_letter_cyber_security.pdf

³ Link to guidance, http://www.sifma.org/newsroom/2014/sifma_publishes_recommendations_for_effective_cybersecurity_regulatory_guidance/

cybersecurity and that cybersecurity is one of many risks that financial institutions and their partners must manage, but can't eliminate.

One such approach is modeled on the NIST Cybersecurity Framework ("NIST Framework") which could provide robust coverage while improving firms' risk posture. The NIST Framework is the preferred starting point for a number of firms in the financial services sector for aligning policy and regulatory oversight. Other financial services firms for whom the NIST Framework is not appropriate still support an approach to cybersecurity regulation which reflects principles of sound risk management.

In specific response to the potential regulations put forward in the letter we submit the following recommendations.

General Recommendations:

As stated in the opening of the letter we view effective cybersecurity guidance and regulation as enabling a covered entity to develop a cybersecurity program that is tailored to its specific situation. Regulations should encourage covered entities to take a risk-based approach, which is customized to the threats they face and takes into account the covered entity's business model and resources available. This approach which is less prescriptive should allow covered entities the flexibility in how they address the guidance from both a policy and technology standpoint and avoid inconsistent or conflicting requirements from other regulators.

Rather than creating another model or method that covered entities should organize around for assessment, development and improvement of their programs, we suggest it would be useful to align any future NYDFS requirements with the NIST Framework as the preferred mechanism. This would help to align policy and regulatory oversight, as well as drive efficiency in the multiple examinations that covered entities are often subject to each year. Coordination is essential to enhance harmonization of regulatory guidance and ensure the most effective use of limited resources. The proliferation of different government security standards creates confusion and fosters an environment which could result in noncompliance.

Providing a uniform approach allows covered entities that straddle different regulators to adopt the same fundamental guidance to developing cybersecurity policies and practices. This will save covered entities from executing multiple audits that cover the same content and shifting resources from security-focused activities. In addition, preparation would be consistent, which allows the reuse of documentation across multiple regulators. Regulators also benefit from sharing solutions to the same compliance problems. Consistency in regulatory guidance creates an environment in which all boats can rise.

Specific Recommendations:

1. **Third-Party Service Provider Management:** Third-party risk management is a critical component to all effective cybersecurity programs. Covered entities should assess and maintain awareness and oversight of parties that they interact and share data with. However, the method of that oversight and influence needs to take into account the limited leverage that covered entities may have with certain vendors and the collaborative relationship that must be established in order to ensure security. The approach to third-party management suggested in the letter using the contract as the primary vehicle for compliance seems prescriptive and potentially impractical. It doesn't account for relationships that are not governed by a formal contract such as relationships with counterparties or participating on an exchange.

The specific requirements to encrypt data in transit and at rest as well as to include indemnifications in the event of losses from incidents and warranties concerning information security are not currently industry practice among most non-financial services companies. In fact, firms have stated that some third-parties are now requesting to include language in contracts that states if the vendor has taken reasonable steps to prevent an information security breach they cannot be held liable if one occurs. We expect very few third-parties would be willing to provide a blanket indemnification or warranties with respect to a cybersecurity breach since this is a risk that can't be eliminated, but must be managed.

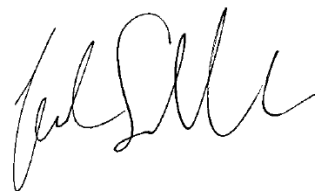
In any event, we seek additional clarity on the meaning and significance of "minimum preferred terms" as used in the NYDFS letter, especially, if such terms cannot be agreed upon. Can a covered entity accept the risk of engaging a third-party that does not agree to the covered entity's terms so long as it incorporates the identified risk into the risk assessment that is performed? Or is it not permitted to engage such third-parties at all? Lastly, there is no guarantee that third-party service providers would agree to the prescriptive requirements of a single state government going forward -- putting covered entities in the difficult position of choosing between severing key ties with third-parties or violating NY DFS regulations. Particularly where suppliers offer hosted multi-client platforms, covered entities located in a single state cannot be expected to wield the commercial leverage necessary to force extraterritorial compliance with that state's requirements. We suggest that regulations should avoid requiring procurement contracts to be the primary means to enforce compliance with security standards. Instead, covered entities should be encouraged to establish or improve upon existing third-party risk management programs to ensure the cybersecurity of their third-parties is assessed and that issues are identified and addressed and the risks of engaging with a specific third-party are understood.

2. Multi-Factor Authentication: The proposal would require multi-factor authentication for all access to internal systems. It is currently typical market practice to employ multi-factor authentication for systems that are exposed to the Internet. To require this control for employees to access internal systems is not typical and is in conflict with existing FFIEC guidance. No one state should demand compliance with a security standard that is inconsistent with Federal requirements. We suggest that covered entities be asked to make use of multi-factor authentication and other enhanced access controls based on the criticality of the system and/or data being accessed. In addition we would advocate for additional clarity around whether covered entities would just be required to make multi-factor identification available to their customers or if they would be required to enforce its usage by all customers.
3. Notice of Cybersecurity Incidents: There are existing notification requirements under NY State law that require a business to disclose any security breach of a system that holds “private information” of New York residents to be reported to those affected New York residents, and to the State Attorney General, the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination. We would ask that any notification requirements for NY DFS be aligned to existing laws and take into account scenarios such as a delay if a law enforcement agency determines that it would impede a criminal investigation.

* * *

SIFMA appreciates the Department’s consideration of the issues and concerns raised above. If you have any questions or require further information, please contact me at (212) 313-1183 (kschimmeck@sifma.org).

Sincerely,



Karl Schimmeck
Managing Director

cc: Shirin Emami, Acting Superintendent of Financial Services