Client Alert

November 18, 2015

NY DFS Signals a Detailed Framework for Cybersecurity Compliance

By Nathan D. Taylor and Adam Fleisher

On November 9, 2015, the New York State Department of Financial Services ("DFS") sent a letter to a number of state and federal financial regulators signaling that DFS may issue comprehensive cybersecurity regulations for financial institutions subject to DFS's authority. The stated purpose of the letter was to "spark additional dialogue, collaboration and, ultimately, regulatory convergence among [the various] agencies on new, strong cyber security standards for financial institutions." Although any cybersecurity regulations issued by DFS would apply only to those financial institutions subject to DFS's authority, DFS is encouraging state and federal financial regulators to work together to develop a comprehensive cybersecurity framework for all financial institutions "in the weeks and months ahead."

DFS'S FINDINGS REGARDING THE STATE OF CYBERSECURITY IN THE FINANCIAL SECTOR

In 2013 and 2014, DFS conducted surveys of various DFS-regulated banking organizations and insurance companies regarding their cybersecurity programs. In response to these surveys, DFS issued reports summarizing its key findings on the state of cybersecurity in the banking sector and the insurance sector and expanded its information technology examination process to "focus more attention on cyber security." As part of this new focus, DFS "began conducting risk assessments of its financial institutions . . . to gather information about industry-wide risks and vulnerabilities."

DFS has drawn a number of conclusions about the state of cybersecurity in the financial sector based on its risk assessments and discussions with various stakeholders. For example, DFS believes that there is a need for financial institutions' cybersecurity programs to remain dynamic in order to keep pace with changes in technology and "the increasingly sophisticated nature of threats." In addition, DFS believes that there is an

Financial Services Regulatory Practice Group

California

Roland E. Brandel	(415) 268-7093
Henry M. Fields	(213) 892-5275
Joseph Gabai	(213) 892-5284

New York

Marc-Alain Galeazzi	(212) 336-4153
Jiang Liu	(212) 468-8008
David H. Medlar	(212) 336-4302
Barbara R. Mendelson	(212) 468-8118
Judy Man Ni Mok	(212) 336-4073
Mark R. Sobin	(212) 336-4222
Joan P. Warrington	(212) 506-7307

Washington, D.C.

Leonard N. Chanin	(202) 887-8790
Meredith M. Cipriano	(202) 887-6936
Rick Fischer	(202) 887-1566
Adam J. Fleisher	(202) 887-8781
Calvin D. Funk	(202) 887-6930
Julian E. Hammar	(202) 887-1679
Ashley R. Hutto-Schultz	(202) 887-1683
Oliver I. Ireland	(202) 778-1614
Donald C. Lampe	(202) 887-1524
Jeremy R. Mandell	(202) 887-1505
Amanda J. Mollo	(202) 778-1609
Obrea O. Poindexter	(202) 887-8741
Ryan J. Richardson	(202) 887-8761
Joe Rodriguez	(202) 778-1610
Sean Ruff	(202) 887-1530
Trevor R. Salter	(202) 887-1527
Nathan D. Taylor	(202) 778-1644

increased reliance on third-party service providers, and such reliance can weaken or render ineffective a financial institution's own cybersecurity protections. DFS also believes that recent security breaches "demonstrate that cyber security is a global concern that affects every industry at all levels."

As a result, DFS has concluded that there is "a demonstrated need for robust regulatory action in the cyber security space." And, DFS is contemplating issuing cybersecurity regulations for financial institutions subject to its authority. In addition, DFS believes that coordination with other state and federal financial regulators would be beneficial in order "to develop a comprehensive cyber security framework that addresses the most critical issues, while still preserving the flexibility to address New York-specific concerns."

THE CONTEMPLATED CYBERSECURITY "FRAMEWORK"

DFS's letter highlights the "key regulatory proposals that [DFS is] currently considering" that would be included in a comprehensive regulatory cybersecurity framework. At a high level, DFS's letter indicates that its potential regulations would require covered financial institutions to maintain a cybersecurity program "designed to perform core cyber security functions." DFS's letter, however, also indicates that its contemplated regulations would require that covered financial institutions take the following steps, "among others":

1) **Policies and Procedures** – Implementing and maintaining a wide range of written policies and procedures addressing twelve broad security concepts, such as data classification, access controls, application management, business continuity and incident response.

2) **CISO** – Designating a Chief Information Security Officer ("CISO") who would be required "to submit to the DFS an annual report, reviewed by the entity's board, assessing the cyber security program and the cyber security risks to the entity."

3) **Vendor Oversight** – Overseeing third-party service providers, including requirements for vendor contracts that address multifactor authentication, encryption, audit and indemnification.

4) **Multifactor Authentication** – Implementing multifactor authentication for online customer access, for internal access to database servers and for remote access.

5) **Logging** – Logging privileged user access and system events and protecting such logs.

6) **Application Security** – Implementing written standards for the security of applications.

7) **Cyber Personnel** – Employing personnel "adequate" to manage cyber risk and perform cyber functions and requiring such personnel to "stay abreast" of changing cyber threats and countermeasures.

8) **Testing** – Conducting annual penetration testing and quarterly vulnerability assessments.

9) **Notice of Incidents** – Providing immediate notice to DFS of cyber incidents that have "a reasonable likelihood of materially affecting" normal operations, including incidents that trigger notice under New York's breach law.

IMPLICATIONS FOR FINANCIAL INSTITUTIONS

Although DFS has not yet issued proposed cybersecurity regulations, DFS's letter clearly signals DFS's intent to do so and in a comprehensive and detailed manner. Although the exact scope and content of any such regulations will not be known until a proposal is issued, there are a number of implications of DFS's letter, both for financial institutions subject to DFS's oversight and for financial institutions subject to the oversight of federal financial regulators.

At a high level, DFS's contemplated regulations do not address new information security concepts. In fact, many of the principles addressed in the contemplated regulations are addressed in existing information security laws and regulations and industry best practices, such as developing and documenting a comprehensive information security program, designating an individual to manage its information security program, training employees and overseeing vendors with access to sensitive information or systems. Nonetheless, DFS's contemplated regulations are significant in their breadth and detail from both an administrative and technical standpoint. For example, the contemplated regulations would require significant administrative controls, including the implementation of a number of specific written policies and procedures, annual reporting to DFS assessing a financial institution's cyber readiness and vendor oversight that includes very specific contractual requirements, such as encryption. In addition, by specifying technical controls, such as multifactor authentication and specific logging requirements, the contemplated regulations deviate from a more traditional risk-based approach where a financial institution must conduct a risk assessment and adopt security controls designed to address those risks.

For financial institutions subject to DFS's authority, such as commercial banks, foreign banks with New York State-licensed offices, money transmitters, mortgage brokers and insurance companies doing business in New York, the contemplated regulations would represent the most detailed and comprehensive cybersecurity standards applicable to those financial institutions under New York law. For example, many financial institutions subject to DFS's authority today may only be subject to limited standards under New York law for the security of information, such as the New York disposal law, requirements to safeguard Social Security numbers or, in the case of New York insurance companies, the more detailed, but still high-level, security standards issued by DFS under the federal Gramm-Leach-Bliley Act ("GLBA"). Even for those financial institutions that operate in other states and that are subject to state safeguards laws that are more detailed than existing New York law, such as the Massachusetts data security regulations and the Nevada encryption requirements, DFS's contemplated regulations would impose significant new obligations, such as multifactor authentication and logging requirements.

Regardless of the substance of any DFS proposal, DFS has made clear that it "considers cyber security to be among the most critical issues facing the financial world today." Beginning with DFS's financial institution surveys in 2013 and its ensuing risk assessments, DFS is focused on identifying cybersecurity risks, deficiencies and areas for improvement. In addition, DFS has expanded its focus on cybersecurity during the examination process. As a result, financial institutions subject to DFS's authority should expect greater scrutiny by DFS of their security practices, regardless of whether DFS actually issues the contemplated regulations. Such financial institutions should monitor DFS's regulatory efforts to prepare to develop a compliance strategy for any such regulations. Those financial institutions may also want to consider the extent to which their existing cybersecurity practices

address the concepts identified in the contemplated regulations. In this regard, DFS has clearly signaled certain principles that it believes are important to a financial institution's cyber preparedness.

For financial institutions that are not subject to DFS's oversight and authority, DFS's letter is also noteworthy. Many financial institutions subject to federal oversight are already subject to requirements and federal agency guidance that are more detailed than DFS's contemplated regulations. For example, the federal banking agencies and the National Credit Union Administration have supplemented their high-level, risk-based GLBA security rules with detailed expectations around information security. In this regard, the Information Security booklet of the Federal Financial Institutions Examination Council highlights agency expectations surrounding a financial institution's information security governance, strategy, risk assessments, controls and monitoring, and it does so in a detailed manner. For example, the Information Security booklet communicates agency expectations for a financial institution's access controls, authentication, remote access, data center security, encryption, system development, personnel security and training, vendor oversight, business continuity, insurance, logging and monitoring and intrusion detection, among others. Nonetheless, financial institutions subject to federal oversight should be mindful that any DFS dialogue with federal financial regulators could lead federal regulators to revisit and potentially supplement or expand their cybersecurity expectations for financial institutions subject to their authority.

Contact:

Nathan D. Taylor
(202) 778-1644
ndtaylor@mofo.com

Adam J. Fleisher
(202) 887-8781
afleisher@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.