Privacy, Data Security &
Information Use

September 28, 2016

New York Sets Uncomfortable Cybersecurity Precedent

By Brian E. Finch and Mercedes K. Tunstall

After much research and discussion, the New York State Department of Financial Services (DFS) has released the near final version of its Cybersecurity Requirements for Financial Services Companies. The DFS Cybersecurity Regulation is breathtaking in its scope and will soon become a major factor in how financial entities, including banks, financial services firms, and insurance carriers secure their operations.

Properly implementing the DFS Cybersecurity Regulation will be no small feat. The regulation requires the implementation of a variety of cybersecurity policies and procedures, ranging from the well-known to the relatively unique. Posing an even greater challenge for entities covered by the regulation is the fact that they must start imposing virtually the same strict cybersecurity controls on third parties with which they do business. It will also require directors and officers of entities falling under its purview to certify annually that they have a compliant program in place. Thus it is easy to anticipate that these newly created or modified cybersecurity programs will be the subject of much scrutiny.

This alert identifies key elements of the DFS Cybersecurity Regulation, which third parties and vendors will be impacted by the Regulation, questions left unanswered by the regulation as currently drafted, and steps covered entities can take to become compliant with the Regulation while also managing potential civil liability.

Overview of the DFS Cybersecurity Regulation

DFS has released one of the most comprehensive and ambitious cybersecurity regulations yet seen. Beginning in 2017, entities covered by the regulation will be required to develop and implement a broad suite of cybersecurity programs and policies, training regimes, risk analyses and vulnerability assessments, incident response capabilities, and other controls. Moreover the regulation requires that the policies, procedures, and various testing programs and assessments be regularly repeated and refreshed. All in all, the regulation represents a significant (and likely costly) set of new requirements for the nearly 2000 covered entities that must comply with it.

The regulation defines covered entities as "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the banking law, the insurance law, or the financial services law." Note that entities are exempted if they have had less than 1,000 customers on average over the past three years, less than $5 million in gross annual revenue in each of the last three fiscal years, and less than $10 million in year-end total assets.

The required elements of the regulation include:

- Designing and implementing a written cybersecurity plan to protect information systems and non-public information (which covers any business-related information, information provided to a covered entity, health care information, and "personally identifiable information"). Some of the more unique cybersecurity plan components include:
    - capacity and performance planning;
    - systems operations and availability concerns;
    - systems and network security and monitoring;
    - systems and application development and quality assurance;
    - physical security and environmental controls; and
    - vendor and third-party service provider management.
- The overall cybersecurity program *shall be reviewed at least annually* by the covered entity's board of directors (or its equivalent governing body,) and approved by a senior officer of the covered entity.
- Creation and implementation of an incident response plan.
- A chief information security officer (CISO) must be appointed and report at least biannually on the state of the entity's cybersecurity to the board of directors or its equivalent.
- Covered entities must either employ cybersecurity personnel or "utilize a qualified third party to assist in complying with the requirements."
- Annual penetration testing and risk assessments must be completed, along with quarterly vulnerability assessments and regular training.
- Cybersecurity audit records must be maintained and kept for at least six years.
- The cybersecurity program must implement security measures for its applications or apps.
- Cybersecurity policies and procedures for third parties doing business with covered entities must be formally documented. Third party security policies must include, at a minimum:
    - Cybersecurity risk assessments of third parties;
    - Specified cybersecurity practices that must be followed by third parties, and due diligence to evaluate the adequacy of the third party's cybersecurity practices;
    - Review and assessment at least once a year of a third party's security procedures;
    - Third party contracting language that requires:

  - The use of multi-factor authentication;
  - Encryption;
  - Prompt notice of cybersecurity events;
  - Right to conduct audits of the third party's cybersecurity posture; and
  - Representations and warranties from the third party service provider that the service or product provided to the covered entity is free of cybersecurity threats.
  - Systems and application development and quality assurance; and
  - Physical security and environmental controls.
- "Cybersecurity events" (defined as "any act or attempt, *successful or unsuccessful*, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system") must be reported to the DFS *no more than 72 hours after their occurrence*. Emphasis added.

The regulation has a 180 day transition period built in to it and covered entities must begin submitting to the superintendent of DFS a "certification of compliance" on January 15, 2018.

Open Questions and Concerns

Some could argue that the regulation constitutes "common sense" cybersecurity measures. While many measures certainly make sense, the challenge for Covered Entities is that the regulation sways between unusually specific and exceedingly vague. Below are a few examples of open questions related to the regulation.

1) Is the definition of "cybersecurity event" intended to be so broad?

As previously discussed, the regulation defines a cybersecurity event as "any act or attempt, successful or unsuccessful" to gain unauthorized access to, disrupt or misuse a covered entity's information system or the information on it. Such events must be reported to the DFS within 72 hours of occurrence.

Based on a plain reading, a "cybersecurity event" constitutes practically any cyberattack, no matter how poorly constructed or executed. No explanation is given regarding what constitutes a "reasonable likelihood" of materially affecting a system, but one can easily imagine the DFS having an unusually broad and permissive definition of "reasonable" in this case.

Covered entities should assume — until proven otherwise — that the DFS will have a penchant for being overly inclusive in considering what constitutes a cybersecurity event. Considering that some entities are subject to hundreds of thousands (if not millions) of attempted cyberattacks on a daily basis, creating a notification process alone could be incredibly burdensome for covered entities.

2) Compliance with third party cybersecurity obligations could be near impossible.

Vendor/third-party security is a critical component of any security program and the DFS was right to address it. Still, the depth of third party cybersecurity obligations is unwieldy to the point where it seems unlikely that any financial institution will actually succeed in ensuring these obligations are met. Especially when dealing with large third party service providers, it may be difficult to obtain all of the requirements in the Regulation.

The most worrisome third party security measure is in Section 500.11(b)(5), which requires covered entities to obtain "representations and warranties from the third party service provider that the service or product provided to the Covered Entity is free of [cybersecurity threats] that would impair the security of the Covered Entity's Information Systems or Non-public Information."

Experience shows that it will be difficult to obtain such a representation, and in any case that such a representation will be useless. Why is that? Because cyber-attacks are omnipresent and it is virtually guaranteed that every system will have some form of malware on it. Studies by companies such as FireEye have repeatedly demonstrated that even the most sophisticated organizations have some form of malware on their system more than 95 percent of the time. As a result, it will be extremely challenging to find a third party that is willing to make the representation required under Section 500.11(b)(5), much less have confidence in such a representation.

Keep in mind too that Section 500.03(a)(10) calls for written policies and procedures related covering "physical security and environmental controls." This requirement could prove equally problematic to implement due to the fact that building landlords, not the covered entities, will likely control those systems. Covered entities will not only have to determine what kinds of cybersecurity policies and procedures will satisfy the section, but also try to figure out a way to get a third party landlord to implement them. That could easily result in significant disputes between the covered entities and property owners, particularly over who is responsible for the significant costs associated with implementing the changes.

3) The Regulation's Definition of "Information Systems" is problematic.

Under the DFS Cybersecurity Regulation, "information systems" are defined to include "electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems."

Despite that lengthy definition, the regulation is still vague as to how far it reaches. For instance, should covered entities consider videoconferencing systems, document management programs and removable storage devices as part of their information system? Time will tell, but the fact remains that more clarification is needed.

4) Insourcing or Outsourcing?

Many covered entities will be able to come into compliance using mostly internal resources. Other companies may elect to use external resources to help comply, as doing so gives them some ability to shift some risk away from the company. There will be some companies that have no choice but to turn almost exclusively to third party service providers to assist with designing and implementing cybersecurity programs. Their decisions will likely be driven by the fact that they do not have the internal resources to fully implement a DFS-compliant cybersecurity program, nor the time to build such a capability.

In each case, the question posed to covered entities is not only how do they decide to outsource their security program but also how doing so can pass muster with DFS. This will be a difficult problem to tackle, in no small part because there are many cybersecurity service providers available but relatively few ways to judge their effectiveness. Moreover, the companies that tend to be better known when it comes to cybersecurity services may be in high demand, thereby raising questions regarding their affordability and availability.

Covered entities that plan to utilize outside resources should immediately begin trying to determine which tasks will be performed by employees and which ones will be handled by contracted parties. They also should consider developing strict vetting and procurement mechanisms to create a record demonstrating a thorough contracting process.

5) Worries for Directors and Officers

Requiring the board to review a company's cybersecurity program is not unusual – indeed many boards are doing so now and are even adding special committees or directors who have specialized knowledge regarding cybersecurity. It is also quite normal to see CISOs and CIOs regularly brief the C-suite and even the board on cybersecurity, as well as to have general counsels and CEOs regularly involved in cybersecurity planning.

However, the requirement in the regulation could impact the design and implementation of a covered entity's cybersecurity program. Simply put, the regulation now puts directors and officers into the position of having to consider a variety of factors beyond whether they have a compliant program in place – they will also have to consider whether the plan meets the amorphous standards set by DFS, as well as whether the plan is "reasonable and adequate." The problem is that there are few to no benchmarks as to whether a cybersecurity plan is "reasonable" or "adequate," especially when one of the presumptions of the underlying regulation is an expectation of perfect security. Perfect cybersecurity does not exist, and so directors and officers should ensure that the plan is sound both technically and legally before any representations are made to DFS.

Using the SAFETY Act To Ease Compliance with the DFS Cybersecurity Regulation.

While the DFS Cybersecurity Regulation is vague in many places, there is a tool covered entities can use right now to help demonstrate a fulsome cybersecurity program — the SAFETY Act. The SAFETY Act (or Support Anti-terrorism by Fostering Effective Technologies Act) is a liability management statute passed into law as part of the Homeland Security Act of 2002.

Under the SAFETY Act, any company that owns, sells or otherwise deploys cybersecurity products, services or policies/programs (including companies that deploy their own cybersecurity policies and programs) may submit an application to the U.S. Department of Homeland Security for specific liability protections, such as a cap on civil damages or immunity therefrom. SAFETY Act protections are only granted if the DHS determines that the policies and programs are useful, effective and have sufficient quality-control mechanisms in place. The review is thorough and the protections granted typically are extended for five years at a time.

Keep in mind that all of the steps and policies that have to be implemented under the regulations (and more) can and will be reviewed by the DHS for SAFETY Act protections. That means a covered entity can seek SAFETY Act protections for its written cybersecurity programs, training programs, risk assessments, and even its vetting processes for third-party vendors. Assuming the covered entity receives a SAFETY Act award, that should serve as very powerful evidence to the DFS that the programs and policies mandated by the regulation are indeed reasonable, have a robust compliance program in place, and are continuously being improved, which are all critical components of receiving SAFETY Act protections.

Remember that holding SAFETY Act protections do not supersede regulatory obligations — the law specifically prohibits using it for such purposes. Still, consider how powerful it will be for a covered entity to come forward with a SAFETY Act-approved cybersecurity program when the DFS inevitably questions its underpinnings.

DFS Cybersecurity Regulation Will Be An Ongoing Challenge

There is no doubt that the New York cybersecurity regulation will be modified and amended. One can also expect that other states will follow with similar regulations, meaning that covered entities are about to face the same bedraggled patchwork of regulatory obligations that it currently faces with respect to data breach notification requirements.

Ultimately, such requirements are here to stay. In the interim, covered entities need to get moving now on compliance programs. The smart ones will work hand in hand with their lawyers to show that they have a reasonable cybersecurity program in place and also examine whether the SAFETY Act can help provide additional evidence of a robust and fulsome cybersecurity program.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the attorneys below.

Brian E. Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Mercedes K. Tunstall (bio)
Washington, DC
+1.202.663.8118
mercedes.tunstall@pillsburylaw.com