New York Law Journal
Technology Today
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 15
TUESDAY, JANUARY 24, 2017

CYBERSECURITY

Amended DFS Regulations Answer Some but Not All Questions

By **Timothy C. Blank**

And **Hilary Bonaccorsi**

The New York State Department of Financial Services (DFS) received numerous comments on its proposed Cybersecurity Requirements for Financial Services Companies (Initial Regulations) and, on Dec. 28, 2016, issued updates to the Initial Regulations (Amended Regulations).[1] The Amended Regulations resolve certain issues, but key questions remain. This article explains why the changes in the Amended Regulations are important to "Covered Entities," and identifies important questions that still need to be resolved.

SHUTTERSTOCK

Initial and Amended Regulations

Both the Initial and Amended Regulations (together, the DFS Regulations) are significantly broader and more prescriptive than any existing cybersecurity regulations. Existing regulations protect *personal* information about individual natural persons, while the DFS Regulations also regulate non-personal business information.[2] This is a big expansion. The DFS Regulations also mandate penetration testing and require that data incidents be reported to DFS within 72 hours.[3] In addition to these new requirements, the Initial Regulations contained significant ambiguities and left key questions unanswered. The Initial Regulations were set to become effective on Jan. 1, 2017.[4]

DFS has now issued Amended Regulations to address comments received from the financial services industry.[5] There is a 30-day comment period during which DFS will review comments that were "not previously made."[6] The Amended Regulations will become effective March 1, 2017, subject to a 180 day grace period and other "Transitional Periods."[7]

Amendments Address Questions

The Amended Regulations resolve a number of the questions commenters raised and now take a more practical approach.

DFS Has Narrowed the Definition of "Nonpublic Information." The Initial Regulations required "Covered Entities" to protect all "Nonpublic Information."[8] The Initial Regulations did not limit "Nonpublic Information" to *personal*

TIMOTHY C. BLANK *is a managing partner at Dechert.* HILARY BONACCORSI *is an associate at the firm.*

information about individuals as with other state and federal regulations.[9] Instead, the Initial Regulations defined "nonpublic information" to include (1) any business-related information that, if tampered with or disclosed, would "cause a material adverse impact to the business, operations or security"; (2) any information an individual provided when obtaining a financial product or service; (3) health-related data; *and* (4) information typically defined as "personal information" such as an individual's name plus his or her Social Security number.[10]

Now, however, the definition of "Nonpublic Information" is more practical. The term is still defined more broadly than in other regulations because it still includes business-related (and not just personal) information.[11] However, DFS has deleted the requirement that "any information" received from an individual in connection with providing a financial product or service be protected.[12] From a compliance perspective, this narrower definition of "Nonpublic Information" will enable "Covered Entities" to more easily identify the data they have that needs to be protected. In addition, because the definition of "Nonpublic Information" flows through to the Updated Regulation's data breach notification requirements, "Covered Entities" will face a smaller pool of data incidents that will potentially need to be reported to DFS.[13]

"Covered Entities" May Now Tailor Their Compliance Programs to Their Specific Risks. The Initial Regulations imposed a blanket "one size fits all" approach to cybersecurity on all "Covered Entities," which was in stark contrast to guidance issued by other financial services regulators who specifically require tailored cybersecurity programs.[14] The Initial Regulations did not provide for flexibility in designing cyber programs to fit a company's risk profile.

The Amended Regulations, however, now provide that "Covered Entities" must conduct a "Risk Assessment" to determine the nature of the "Nonpublic Information" they hold and the risks associated with that information.[15] From a compliance standpoint, the "Risk Assessment" will limit some "Covered Entities'" obligations under the Amended Regulations as certain other provisions now no longer apply across-the-board, but rather only to the extent applicable based on the "Risk Assessment." And, from a practical standpoint, conducting a risk assessment generally allows industry participants to truly understand the information they hold and the risks to their businesses. This in turn allows for effective cybersecurity programs rather than programs based on template policies that are drafted to "check the boxes" mandated by a given regulation. As a result, the Amended Regulations have now moved more in line with other financial regulators' approach to creating tailored cybersecurity policies.

> The Amended Regulations resolve a number of the questions commenters raised and now take a more practical approach.

The 72-Hour Notice Period Remains, but There May Be Fewer Reportable Events. The notification provision under which "Covered Entities" were required to report to DFS all "Cybersecurity Events" that affected "Nonpublic Information" within 72 hours of discovery was heavily criticized. Because of the broad definition of "Cybersecurity Event," which includes "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System" and the expansive scope of information that was previously considered "Nonpublic Information," industry participants argued that the reporting requirements "would result in many reports that are of little cybersecurity value."[16]

In response, DFS has limited the definition of "Nonpublic Information" so that notice to DFS of cybersecurity events is required only when notice is already being provided to another government or supervisory body or when a materiality threshold is met.[17] DFS retained the 72-hour requirement, but the clock begins to run once a *determination* has been made that the event is reportable.[18] This is a far more practical approach, and will eliminate the need to report immaterial or "de minimus" cyber events.

Key Issues Remain Unresolved

DFS has addressed many of the issues in the Initial Regulations, but there are key questions that remain unanswered.

It Remains Unclear to Whom the Amended Regulations Apply. The Amended Regulations do not explicitly list the types of entities to which they apply.[19] A key question has been whether the Updated Regulations apply to SEC registered investment advisers (Advisers). The Initial Regulations defined a "Covered Entity" 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."[20] The Amended

Regulations only revised the definition to reference the "Banking Law," the "Insurance Law" and the "Financial Services Law" in capitalized terms.[21] The introductory provisions to the New York State Banking Law, Insurance Law and Financial Services Law, respectively, explain that each can be referred to in shorthand as they are in the Amended Regulations, but each law is ambiguous about the entities it covers.[22]

Information on the DFS website, however, is instructive as to whether Advisers are covered. DFS does not include Advisers in its list of the types of entities it supervises.[23] In addition, a search for all entities supervised by DFS returns a comprehensive list that does not identify a single Adviser.[24] As a result, while DFS has not explicitly listed the entities to which the Amended Regulations apply, it appears that the Amended Regulations are not intended to apply to Advisers.

The Scope of Liability Has Not Been Addressed. DFS has not addressed the scope of liability for a violation of the Amended Regulations. In certain situations, DFS can impose penalties such as fines when taking disciplinary actions against entities it regulates.[25] However, despite the requirement that the Chairperson of the Board of Directors submit a Certification of Compliance to DFS on an annual basis, DFS has not addressed whether it can or will impose personal liability on such officers.[26]

Certain "Transitional Periods" for Compliance Are Contradictory. To address concerns about the original implementation timeframes, DFS added "Transitional Periods" of one to two years for compliance with certain provisions.[27] In doing so, DFS gave "Covered Entities" one year to conduct their "Risk Assessments."[28] However, "Covered Entities" have only 180 days to become compliant in certain areas that can only be identified during the "Risk Assessment." For example, within 180 days, "Covered Entities" are required to have a Cybersecurity Program and Cybersecurity Policy, both of which "shall be based on the Covered Entity's Risk Assessment."[29] Clearly the information learned by a "Covered Entity" during its "Risk Assessment" will be crucial to developing effective programs and policies, and therefore DFS should harmonize the timeframes for compliance.

Conclusion

The Amended Regulations are still much broader than existing information security regulations, though the Amended Regulations are significantly more practical then the Initial Regulations. In particular, the requirement that "Covered Entities" (a term which appears not to include Advisers) tailor cybersecurity programs to a "Risk Assessment" will make those programs much more effective. In addition, many of the compliance steps required to be taken under the Amended Regulations are already proven best practices in the industry. The Amended Regulations do create the risk of an enforcement action and thus compliance should be viewed as an opportunity for industry participants to take all appropriate steps to ensure cyber readiness.

1. See "DFS Issues Updated Proposed Cybersecurity Regulation Protecting Consumers and Financial Institutions," New York Department of Financial Services Press Release, December 28, 2016, available at http://www.dfs.ny.gov/about/press/pr1612281.htm (hereinafter Dec. 28, 2016 Press Release).
2. See, e.g., Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00 (2010); but see Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500.00 (2016) (hereinafter Amended Regulations).
3. Amended Regulations §500.05.
4. Cybersecurity Requirements for Financial Services Companies, Vol. No. XXXVIII, N.Y. Reg. Sept. 28, 2016.
5. Dec. 28, 2016 Press Release.
6. Id.
7. Amended Regulations §§500.21-500.22.
8. Cybersecurity Requirements for Financial Services Companies, New York State Department of Financial Services Proposed 23 NYCRR 500, Sept. 13, 2016 at 2 (PDF only) (hereinafter Initial Regulations).
9. Id.
10. Id.
11. Amended Regulations §500.01(g).
12. Id.
13. Amended Regulations §500.17.
14. See, e.g., National Exam Program Risk Alert, "OCIE's 2015 Cybersecurity Examination Initiative, Sept. 15, 2015, available at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.
15. Amended Regulations §500.09.
16. Amended Regulations §500.1(d); Assessment of Public Comments for New Part 500 to 23 NYCRR, available at http://www.dfs.ny.gov/legal/regulations/proposed/rp500apc.pdf.
17. Amended Regulations §500.17.
18. Id.
19. Amended Regulations §500.01(c).
20. Initial Regulations at 2-3.
21. Amended Regulations §500.01(c).
22. See, e.g., NY Fin. Serv. Law §§101, 104.
23. New York State Department of Financial Services, "Who We Supervise," available at http://www.dfs.ny.gov/about/whowesupervise.htm (last visited Jan. 17, 2017).
24. Id.
25. See, e.g., New York State Department of Financial Services Takes Disciplinary Actions Against Companies, Agents, Brokers & Adjusters, Jan. 6, 2017, available at http://www.dfs.ny.gov/insurance/da/2011–2020/da20170106.pdf.
26. Amended Regulations §500.00.
27. Amended Regulations §500.22.
28. Id.
29. Id.