Davis Polk

New York DFS issues guidance for adoption of affiliates' cybersecurity programs

November 3, 2021 | Client Update | 3-minute read

The New York DFS issued new guidance regarding a covered entity's reliance on an affiliate's cybersecurity program. The guidance explains DFS's view that, when a covered entity relies on an affiliate's program, DFS has authority to examine the affiliate's program.

Since 2017, New York's Cybersecurity Regulation, 23 N.Y.C.R.R. Part 500, has required any "Covered Entity"—that is, any entity regulated by New York's Department of Financial Services (DFS)—to maintain a risk-based cybersecurity program consistent with certain prescriptive technical and procedural requirements. These requirements, the DFS has maintained, are designed to ensure that the Covered Entity's program adequately protects the Covered Entity's information systems and the nonpublic information maintained on them.

The Cybersecurity Regulation allows a Covered Entity to meet its own obligations by adopting, in whole or in part, the cybersecurity program of an affiliate. *See* 23 N.Y.C.R.R. § 500.2(c). But there has been significant uncertainty as to consequences of the decision by a Covered Entity to adopt an affiliate's cybersecurity program—for both the Covered Entity and the affiliate. It has been unclear (a) what accountability or responsibility the Covered Entity would be assuming with respect to the affiliate's program, and (b) what oversight or examination authority the DFS would assert with respect to the affiliate's program. The issue has been particularly sensitive for a Covered Entity that is a small part of a larger organization and relies on components of the larger entity's cybersecurity program. In short, does this reliance bring the larger entity's program within the scope of a DFS examination, even if that entity is not otherwise regulated by DFS?

The new guidance states that a Covered Entity may rely on an affiliate's program but may not delegate responsibility for compliance with the Cybersecurity Regulation to its affiliate. In the guidance, DFS states that it may examine the adopted portions of the affiliate's cybersecurity program to ensure that the Covered Entity is in compliance with the Cybersecurity Regulation, even if the affiliate is not regulated by DFS.

To enable DFS's examination and supervision, the guidance states that Covered Entities must make available to DFS, upon request, all "documentation and information" sufficient to show that the adopted cybersecurity program complies with the Cybersecurity Regulation. *See* 23 N.Y.C.R.R. § 500.2(d). The guidance states that, at a minimum, the Covered Entity must provide DFS with access to "documentation including the affiliate's cybersecurity policies and procedures, risk assessments, penetration testing and vulnerability assessment results, and any third party audits that relate to the adopted portions of the cybersecurity program of the affiliate." The guidance suggests that Covered Entities should enter binding contractual agreements with their affiliates as needed to ensure they are able to provide DFS with the information and access needed to perform any required supervision and examination.

Takeaways

There are a few important takeaways from this guidance:

1. While a Covered Entity may comply with its obligations under DFS's Cybersecurity Regulation by adopting an affiliate's cybersecurity program, the Covered Entity will be responsible for ensuring that the relevant aspects of the adopted program independently satisfy the Cybersecurity Regulation's minimum requirements.

2. Covered Entities should work with affiliates—in advance—to clearly define the scope of any such adoptions, and to identify the process that the Covered Entity will undertake to ensure compliance with the Cybersecurity Regulation (including the records and information that the Covered Entity will receive and review as part of that process).

3. Both Covered Entities and their affiliates should anticipate that DFS examiners will seek to review any aspect of the affiliate's cybersecurity program that the Covered Entity has adopted, even if DFS does not regulate the affiliate.

4. The Covered Entity should ensure that it has an agreement with its affiliate to permit the Covered Entity to access necessary documentation and information and to provide such documentation and information to the DFS as part of the supervisory examination process.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Greg D. Andres
+1 212 450 4724
greg.andres@davispolk.com

Matthew J. Bacal
+1 212 450 4790
matthew.bacal@davispolk.com

Martine M. Beamon
+1 212 450 4262
martine.beamon@davispolk.com

Angela T. Burgess
+1 212 450 4885
angela.burgess@davispolk.com

Robert A. Cohen
+1 202 962 7047
robert.cohen@davispolk.com

James W. Haldin
+1 212 450 4059
james.haldin@davispolk.com

Daniel E. Newman
+1 212 450 4992
daniel.newman@davispolk.com

Gabriel D. Rosenberg
+1 212 450 4537
gabriel.rosenberg@davispolk.com

Margaret E. Tahyar
+1 212 450 4379
margaret.tahyar@davispolk.com