Articles + Publications | January 24, 2022

New NY DFS Cyber Reg FAQs: Novel Approach to Notifications on Vendor Breaches; Cloud and Other Services Are Part of "Internal Networks" and No Specific Framework Required for Risk Assessment

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos

The New York Department of Financial Services (the "NY DFS") has published three new FAQs that interpret certain requirements under its Cybersecurity Regulation (23 NYCRR 500, the "NY DFS Cyber Reg") related to breaches by service providers, the use of cloud and other services, and risk assessments. The NY DFS FAQs are available at FAQs: Cybersecurity Filing | Department of Financial Services (ny.gov)

Notifications of Service Provider Breaches. The first of these new FAQs will change the way NY DFS licensees report cybersecurity events. Typically, when service providers (including HIPAA business associates) experience a reportable cybersecurity event, the required notices to state and federal agencies are commonly provided by the service provider on behalf of the service provider's customers. In many cases, this approach avoids dozens, hundreds or more notices by the data owners or licensees of the same incident to the same agencies. Also, the service provider has the factual information concerning the incident, and the data owner or licensee has only the information provided by the service provider with no independent way to determine the basic information concerning the event.

FAQ 39 asks, "When there is a Cybersecurity Event at a Third Party Service Provider that affects a Covered Entity, is that Covered Entity required to notify DFS even if the Third Party Service Provider notifies DFS on the Covered Entity's behalf?" In answering the question, the NY DFS states that "the Covered Entity itself must provide notice to DFS directly – regardless of whether the Third Party Service Provider . . . offers to provide notice on the Covered Entity's behalf."

Therefore, the NY DFS has taken the novel position that its covered entities must provide notice of reportable cybersecurity events, and cannot delegate that responsibility to the service provider.

Internal Networks include Cloud Services. In FAQ 40, the NY DFS states that cloud-based email, document hosting and related services are considered to be part of the internal networks of the covered entity, so multi-factor authentication is required to access these facilities as though they were on-premises.

Cyber Assessment Frameworks. According to FAQ 41, the NY DFS Cyber Reg requires comprehensive risk assessments, but they do not need to comport with any particular standard or framework. Covered entities are expected "to implement a framework and methodology that best suits their risk and operations." Even so, the NY

DFS references the “widely used frameworks” of the Federal Financial Institutions Examination Council Cyber Assessment Tool, the Cyber Risk Institute Profile, and the National Institute of Standards and Technology Cybersecurity Framework.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber