CARLTON FIELDS

DFS Continues Focus on Cybersecurity: Issues Ransomware Guidance and Signals Increased Enforcement Actions

CYBERSECURITY AND PRIVACY | FINANCIAL SERVICES REGULATORY | TECHNOLOGY | WHITE COLLAR CRIME & GOVERNMENT INVESTIGATIONS | JULY 15, 2021


Joseph W. Swanson


Michael L. Yaeger


Patricia M. Carreiro

The New York State Department of Financial Services (DFS) is continuing its focus on financial institutions' cybersecurity, issuing new guidance, probing cybersecurity as part of routine examinations, and signaling increased enforcement actions. All of this comes amid a spate of high-profile ransomware attacks in recent months, including some involving financial institutions.

Here is what financial institutions need to know in light of these developments:

- On June 30, 2021, DFS, reporting a 300% increase in ransomware attacks in 2020 and recognizing that "ransomware attacks continue to surge … [and are] jeopardizing the stability of the financial services industry," issued new ransomware guidance stressing "key cybersecurity measures to reduce [the] risk of ransomware attacks." The measures, many of which overlap with guidance issued by the White House in June (and reported by us here), included employee training, vulnerability and patch management, password policies, multifactor authentication, access limitations, system monitoring, backup systems, and tested incident response plans.
- DFS has made probing entities' compliance with Part 500's cybersecurity requirements a standard part of routine examinations, requesting evidence of practices such as risk assessments, third-party service provider oversight, and general cybersecurity governance.
- DFS has brought multiple enforcement actions against entities as a result of these examinations, including those that allegedly failed to report cybersecurity events within 72 hours or to implement multifactor authentication. Fines have cost these companies millions of dollars, as well as the cost of independent consultants to audit and oversee their compliance programs, which is often required as part of resolving the enforcement actions.

Failing to comply with Part 500 can expose the company and its leadership to hefty fines and costly class action litigation. For example, New York Banking Law penalizes "unsafe or unsound" cybersecurity practices at up to $250,000 per day, and life insurance companies are subject to penalties of up to $1,000 per violation of Part 500. Lastly, the board or senior official providing Part 500's required annual certification of their entity's compliance with Part 500, if their statement is incorrect and intentionally made, may be charged with a Class A misdemeanor.

Given the above, financial institutions should reexamine their compliance with Part 500's cybersecurity requirements and ensure they can promptly demonstrate their compliance to regulators. Not only does this work mitigate compliance risk, but implementing these measures should also reduce the organization's risk of an attack in the first place.