BakerHostetler

New York Brings Long-Awaited Cybersecurity Message Case

By Jonathan A. Forman and Eulonda G. Skyles

Jonno Forman is a partner with BakerHostetler in New York. He is an experienced litigator and compliance attorney who guides financial services and emerging technology clients through ever-changing federal and state regulations. Eulonda Skyles is a partner with BakerHostetler in Washington, D.C. She is an accomplished technology attorney with extensive experience in privacy and data security, intellectual property and complex tech licensing transactions. Contact: jforman@bakerlaw.com or eskyles@bakerlaw.com.

Ever since the New York State Department of Financial Services ("DFS") instituted its first-in-the-nation Cybersecurity Regulation[1] in 2017,[2] banks, insurance companies, and others in the financial services industry wondered what would trigger an enforcement action under its broad purview. At long last, the industry now knows. On July 22, 2020, the DFS announced[3] a statement of charges against First American Title Insurance Company ("First American") alleging violations of the regulation for not properly safeguarding customer information. Because First American stated it will contest these charges at a hearing scheduled for October 2020, the industry will have to wait a little longer for more concrete guidance from this proceeding, including the potential consequences of not complying with the regulation. Nevertheless, the allegations in the statement of charges still provide the clear message that the DFS is now enforcing this regulation against perceived violators.

Cybersecurity Regulation

By way of background, the Cybersecurity Regulation is a data privacy and business continuity regulation that seeks to protect New Yorkers by safeguarding the information systems of DFS licensees and the nonpublic information (broadly defined to include trade secrets, personally identifiable information, and personal health information) residing on those systems. To that end, the regulation obligates licensees to implement a cybersecurity program informed by periodic risk assessments, documented by written policies and procedures, and overseen by a designated Chief Information Security Officer who reports directly to the board of directors or senior management. The regulation also requires licensees to, among other things:

- Conduct penetration testing and vulnerability assessments.
- Utilize multi-factor authentication ("MFA") and encryption as appropriate.
- Maintain an audit trail to support normal operations and detect cybersecurity events.
- Limit access privileges as necessary.
- Implement protocols on application security and use of third-party service providers.
- Annually certify compliance with the regulation to the DFS and notify the Superintendent of any cybersecurity events.
- Although the Cybersecurity Regulation provides some limited exemptions from these requirements, it is an expansive regulation that reaches beyond New York's borders. In fact, many licensees are domiciled elsewhere but still must comply with the regulation because they have some operations in the Empire State.

Statement of Charges

The yet-to-be-tested statement of charges paints an unflattering picture of First American's cybersecurity program, alleging that a vulnerability on its public website over several years exposed millions of documents containing consumers' sensitive personal information, including bank account numbers, mortgage and tax records, Social Security numbers, wire transaction receipts, and drivers' license images. According to the statement of charges, the vulnerability exposed this sensitive information to anyone with a web browser. The DFS also alleges that First American failed to promptly remedy this unauthorized exposure after it was discovered in a December 2018 penetration test, noting the following missteps allowed the vulnerability to persist for years—and even for months after it was discovered:

- Neglecting to follow the recommendations of its own cybersecurity team to respond to the vulnerability "as soon as possible."
- Not following its own policies, which required it to conduct a security review and a risk assessment of the vulnerability and the exposed information.
- Misclassifying the vulnerability as "medium" or "low" severity and failing to investigate the vulnerability within its own defined time period.
- Failing to conduct a reasonable investigation into the scope and cause of the exposure after it was reported by a third party.
- Assigning remediation to a new employee who had little data security experience, with little guidance about the severity of the vulnerability.

This article was originally published in the September 2020 issue of Wall Street Lawyer.

- Not implementing centralized and coordinated training to protect against the unauthorized exposure of sensitive information.

In all, the DFS alleges that First American violated the following provisions of the Cybersecurity Regulation:

- 500.02—requiring a cybersecurity program informed by a risk assessment.
- 500.03—requiring written policies approved by a senior officer or the board of directors.
- 500.07—requiring access controls.500.09—requiring periodic risk assessments.
- 500.14(b)—requiring regular training.
- 500.15—requiring encryption in transit and at rest.

The statement of charges seeks findings on these alleged violations and on whether a civil monetary penalty or other relief should be imposed. Because the DFS alleges that each instance of nonpublic information in the charges constitutes a separate violation, carrying up to $1,000 in penalties per violation, the potential civil penalty here could be staggering given the millions of allegedly exposed documents. Indeed, this case sends a clear message to DFS licensees of all sizes about the importance the DFS places on maintaining a cybersecurity program that properly addresses the risks of a business's operations and reasonably responding to and remediating data breaches and other cybersecurity events as they occur.

ENDNOTES:

[1] 23 NYCRR Part 500.

[2] *See* https://www.bakerdatacounsel.com/cybersecurity/beware-the-ides-of-march-is-your-nydfs-cybersecurity-compliance-in-order/.

[3] https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221.

This article was originally published in the September 2020 issue of Wall Street Lawyer.