PUBLICATION

Lessons Learned from the NYDFS First Cybersecurity Regulation Enforcement Action

Authors: Matthew George White, Alexander Frank Koskey, III
July 29, 2020

Last week, the New York Department of Financial Services (NYDFS) filed its first enforcement action against a title insurance company (the company) alleging multiple violations of its Cybersecurity Regulation. New York's Cybersecurity Regulation was passed in 2017 and requires banks, insurance companies, and other financial institutions to establish and maintain a rigorous cybersecurity program. The action is a clear warning from the NYDFS to financial institutions to pay attention to the Cybersecurity Regulation's requirements for their data security programs, and that failures to do so may spawn enforcement actions.

Allegations:

The NYDFS alleges that the company "exposed tens of millions" of documents between 2014 and 2019, which contained sensitive personal information, including Social Security numbers, bank account numbers, mortgage and tax records, and drivers' license images. As of May 2019, the database allegedly contained over 850 million documents spanning more than 16 years. According to the NYDFS, the sensitive personal information was contained in a data storage system that due to a flaw became accessible to the public through a website without any login or authentication requirements. The Notice of Charges states that the company discovered the vulnerability during penetration testing in December 2018 but did not correct the issue for another six months.

The company issued a statement that it "strongly disagrees" with the allegations made by NYDFS and that it would contest the charges. Additionally, the company stated its primary regulator reviewed its response to the incident and found it to be sufficient, and that in May 2019 an outside consultant found that only a limited number of documents were at risk and none belonged to New York customers.

Under the Cybersecurity Regulation, each exposure of personal information is considered a separate violation with a penalty of $1,000 each. Therefore, the potential fines that could be imposed upon the company are massive.

Takeaway:

The NYDFS Cybersecurity Regulation represents the most onerous data security regulation directed specifically toward the financial services industry. It includes requirements to:

- perform adequate risk assessments,
- employ proper data governance and classification,
- ensure the security of information maintained or accessed by third parties,
- conduct periodic penetration testing, and
- provide adequate training to employees, among many other requirements.

In addition, the Cybersecurity Regulation includes requirements for incident response planning and notification requirements.

If your company is subject to the Cybersecurity Regulation, this enforcement action is a good reminder to make sure that your cybersecurity program is compliant with its requirements and is specifically designed to meet the numerous obligations imposed under the Regulation. In addition, this action demonstrates that the NYDFS will review a company's decisions and actions when faced with an incident and may not defer to determinations made by other regulators. Accordingly, it is important that you have a well-established incident response plan, that you involve counsel in the preparation and implementation of that plan, and that you are prepared to defend your actions to the NYDFS when an incident occurs. As demonstrated by the allegations in this enforcement action, the failure to do so could result in significant fines.

If you have any questions regarding the NYDFS Cybersecurity Regulation, or any data privacy or cybersecurity issues affecting the financial services industry, please contact the authors of this article, or any member of Baker Donelson's Data Privacy and Cybersecurity team.