WINSTON & STRAWN LLP

BLOG

NY Department of Financial Services Brings First Cybersecurity Enforcement Action

AUGUST 13, 2020

The New York Department of Financial Services (NYDFS) has announced its first enforcement action under New York's recently effective financial services cybersecurity regulation (23 NYCRR Part 500) (the "Cybersecurity Regulation"). The NYDFS alleged that the target, a bank and title insurance company, had a "known vulnerability" which resulted in the exposure of millions of documents containing sensitive personal information. This information allegedly included consumers' bank account numbers, Social Security numbers, other government ID numbers, and mortgage and tax records. NYDFS alleged that the company first discovered this vulnerability in December 2018, but did not act quickly to investigate and remediate the issue.

The specific failures cited by NYDFS include allegations that the company:

- failed to follow its own policies, neglecting to conduct a security review and a risk assessment of the flawed computer program and the sensitive data associated with the data vulnerability;
- misclassified the vulnerability as "low" severity despite the magnitude of the document exposure, while also failing to investigate the vulnerability within the timeframe dictated by First American's internal cybersecurity policies;
- failed to conduct a reasonable investigation into the scope and cause of the exposure after discovering the vulnerabilities in December 2018, reviewing only 10 of the millions of documents exposed and thereby grossly underestimating the seriousness of the vulnerability; and
- failed to follow the recommendations of its internal cybersecurity team to conduct further investigation into the vulnerability.

On the basis of these purported vulnerabilities, NYDFS brought the enforcement action alleging six violations of the Cybersecurity Regulation. The Cybersecurity Regulation carries a penalty of up to $1,000 per violation. This enforcement action provides guidance to companies who fall under the NYDFS jurisdiction as to expectations of cybersecurity controls and appropriate response in the event of a data breach.

TIP: With the Cybersecurity Regulation now in full effect, any organization covered by the law must implement the required cybersecurity controls, including appointing a CISO, implementing a written information security policy, undergoing regular risk assessments, and following cybersecurity response plans. For more information on compliance with the Cybersecurity Regulation, please see our previous blog post on this topic.

1 Min Read

Author

Eric Shinabarger

Related Locations

Chicago | Houston

Related Topics

Consumer Privacy | Data Breach

Related Capabilities

Privacy & Data Security | Financial Services

Related Regions

North America

Related Professionals

Eric Shinabarger

Alessandra Swanson

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.