July 30, 2020

New York DFS Files First Enforcement Action Alleging Violations of Cybersecurity Regulation

On July 22, 2020, the New York State Department of Financial Services ("DFS") filed its first enforcement action based on alleged violations of its Part 500 Cybersecurity Regulation ("Part 500"). The action alleges that First American Title Insurance Company, one of the largest title insurance providers in the United States, violated Part 500 when it failed to adequately protect its data and exposed hundreds of millions of documents, millions of which contained consumers' sensitive personal information, to unauthorized parties over the course of several years. Notably, in the notice of charges, DFS particularly faults the company's response upon first learning of the issue. The charges show that DFS conducted an extensive investigation, including interviews of the company's CISO and other personnel. The charges will be heard at a DFS administrative hearing. First American issued a statement disputing the allegations.

Background

Promulgated in 2017 and fully effective as of March 1, 2019, Part 500 requires covered financial institutions in New York to establish and maintain cybersecurity programs designed to protect consumers and the financial services industry from the threat of cyberattacks. DFS proposed Part 500 in September 2016, after conducting a survey of the cybersecurity practices of some 200 regulated banking institutions and insurance companies and meeting with industry experts. Part 500 has since been used as a model for other regulators seeking to implement industry-specific cybersecurity guidelines, including the U.S. Federal Trade Commission, multiple states, and the National Association of Insurance Commissioners.[1]

Among other things, Part 500 requires covered institutions to designate a Chief Information Security Officer ("CISO"), enact a comprehensive cybersecurity policy and incident response plan, implement a reporting system for cybersecurity incidents, and file an annual certification confirming compliance with the regulations.[2] Violations of Part 500 can carry penalties of up to $1,000 per violation, with each instance of disclosure of nonpublic information constituting a separate violation.[3] In May 2019, DFS established a new Cybersecurity Division to issue guidance, conduct cyber-related investigations, and enforce Part 500 as appropriate.

Enforcement Action

DFS's first enforcement action under Part 500 comes roughly a year and a half after First American Title Insurance Company ("First American") discovered a vulnerability in its information systems in December 2018. The vulnerability, which arose after a software update to one of First American's document delivery

systems, essentially allowed any individual with whom First American shared a single document in the course of a real estate transaction to access all documents in its delivery system, regardless of whether they were authorized to do so. Many such documents even made their way onto Google's open-source search platform and could be publicly accessed as a result of the vulnerability. This allegedly led to the exposure of millions of consumers' sensitive personal information over the course of several years, from at least October 2014, when the software update occurred, through May 2019, when First American remediated the vulnerability. The sensitive information exposed included bank account numbers, mortgage and tax records, Social Security numbers, wire transaction receipts and drivers' license images.[4]

DFS alleges that, notwithstanding the broad scope and potential significance of this vulnerability and resultant data breach—both of which were highlighted by First American's cyber defense team in its initial internal report—First American failed to adequately investigate or remedy the vulnerability upon discovering it, instead allowing "unfettered access to the personal and financial data of millions of its customers for six more months until the breach and its serious ramifications were widely publicized by a nationally recognized cybersecurity industry journalist." In particular, and in what the DFS refers to as a "cascade of errors" by First American's management, First American allegedly appointed a new employee with little experience in data security to remediate the vulnerability, incorrectly classified the vulnerability and breach as "medium" severity before accidentally downgrading it to "low" severity, reviewed only ten of the millions of documents exposed as a result of the breach, and otherwise failed to follow its written policies and the advice of its cyber defense team.[5]

As a result of these alleged inadequacies, DFS contends that First American violated six provisions of Part 500, including provisions requiring covered entities to perform regular data security risk assessments (500.02 and 500.09), maintain and follow written data security policies (500.03), limit user access privileges to systems housing consumer data (500.07), provide regular cybersecurity awareness training to employees (500.14), and implement encryption and other controls to protect consumer data (500.15).[6]

DFS seeks civil monetary penalties against First American as a result of these alleged violations, as well as an order requiring it to remedy its allegedly deficient cybersecurity program.[7]

Implications

DFS's creation of a new Cybersecurity Division in 2019 seemed to signal an intent "to vigorously enforce and examine compliance with its groundbreaking cybersecurity regulations," as Paul, Weiss wrote at the time.[8] Its recent enforcement action confirms that understanding, and suggests that the new Division is committed to taking action when covered entities fail to promptly identify and address vulnerabilities in the systems they use to house consumer data, as required under Part 500. (By contrast, DFS has not yet taken a public enforcement action under its Part 504 regulations, which impose sanctions and AML requirements on covered entities and also require annual compliance certifications.)

DFS's enforcement action against First American underscores the need for New York-regulated insurance companies and other covered entities to review their cybersecurity programs and policies regularly to ensure they meet Part 500's strict requirements. Should they experience a data breach or other incident of unauthorized exposure, such entities should also ensure that they act promptly to implement remediation.

More broadly, it is notable that this enforcement action is a contested notice of charges, rather than a settled consent order, perhaps indicating an increased willingness by DFS to file contested charges; currently, charges are also pending against Mallinckrodt PLC and Endo International PLC for opioid-related conduct.[9] If the hearing against Mallinckrodt takes place in August as scheduled, it would be the first significant contested DFS hearing.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Michael E. Gertzman
+1-212-373-3281
mgertzman@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Associate Julie L. Rooney contributed to this client memorandum.

---

1 NY DFS Press Release, *Department of Financial Services Announces Cybersecurity Charges Against a Leading Title Insurance Provider for Exposing Millions of Documents with Consumers' Personal Information* (July 22, 2020), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221.

2 *Id.*

3 *Id.*

4 *Id.*

5 *Id.*

6 NY DFS, *In re First American Title Ins. Co.*, No. 2020-0030-C (July 21, 2020), https://www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf.

7 *Id.*

8 Paul, Weiss Client Alert, *New York DFS Creates new Cybersecurity Division* (May 29, 2019), https://www.paulweiss.com/practices/litigation/data-innovation-privacy-cybersecurity/publications/new-york-dfs-creates-new-cybersecurity-division?id=28802.

9 Paul, Weiss Client Alert, *NY DFS Files Enforcement Action against Opioid Manufacturer for Insurance Fraud* (May 1, 2020), https://www.paulweiss.com/practices/litigation/white-collar-regulatory-defense/publications/ny-dfs-files-enforcement-action-against-opioid-manufacturer-for-insurance-fraud?id=36548.