SULLIVAN & CROMWELL LLP

July 31, 2020

New York State Department of Financial Services Announces First Enforcement Action Under Cybersecurity Regulations

Action Against Title Insurance Company Based on Asserted Failure to Protect Tens of Millions of Documents Containing Sensitive Consumer Information

SUMMARY

On July 22, 2020, the New York Department of Financial Services ("DFS") announced an enforcement action seeking monetary penalties and injunctive relief against First American Title Insurance Company ("First American") for purportedly violating six provisions of DFS's cybersecurity regulations, 23 NYCRR Part 500 ("Regulations"). DFS alleges that a vulnerability in First American's public-facing website and information systems caused tens of millions of documents containing consumers' personal information to be publicly available over the course of several years. Moreover, First American allegedly discovered the vulnerability in December 2018 but failed to promptly remedy it, permitting unauthorized access to the consumer data to continue until May 2019, when details of the breach were publicized. These charges represent the first time that DFS has sought to exercise its enforcement powers under the Regulations, which took partial effect in March 2017 and became fully effective in March 2019, and may signal DFS's intention to more actively enforce the Regulations going forward. In its press release, DFS takes the position that each instance of non-public information ("NPI") encompassed by the charges counts as a separate infraction under the Regulations, each of which carry up to $1,000 in penalties per violation, indicating that DFS may seek to impose very significant financial penalties in connection with data breaches compromising large amounts of NPI.

BACKGROUND

According to the Statement of Charges filed by DFS against First American,[1] when consumers apply to purchase title insurance from First American, the company collects consumers' NPI from a number of different sources. First American stores documents containing such NPI in a repository known as "FAST," and its employees can share documents from FAST with third parties, such as parties to a real estate transaction, using an application called "EaglePro." EaglePro provides recipients a URL web link that, without any authentication requirement, permits access to shared documents. An October 2014 update to EaglePro allegedly introduced to the shared URLs an "ImageDocumentID" number that corresponds to the particular document from FAST being shared. Because documents in FAST were assigned sequentially numbered ImageDocumentIDs, a recipient of an EaglePro URL web link could view other FAST documents by simply altering the digits of the ImageDocumentID in the URL. According to DFS, this effectively permitted anyone in possession of any URL generated by EaglePro access to all of the approximately 850 million documents in the FAST database, many of which contained consumer NPI.

DFS alleges that a December 2018 internal cybersecurity test alerted First American to this vulnerability, but the company failed to take appropriate steps to remedy the problem in a timely fashion, allowing the vulnerability to persist until a journalist publicly identified the issue on May 24, 2019.

According to DFS, a "cascade of errors" contributed to First American's security lapse and allowed it to persist for six months after First American learned of the issue. First, the title insurer allegedly ignored that its procedure for classifying documents that contained NPI within FAST—which relied on manual tagging and an instruction to employees not to distribute NPI documents—was "significantly flawed." Then, following detection of the problematic URLs in December 2018, First American purportedly reviewed only a "preposterously minimal" sample of 10 documents exposed by the vulnerability, none of which contained NPI. This led the company to mistakenly conclude that NPI was not affected, causing First American to erroneously classify the breach as "medium severity." First American's misdiagnosis was allegedly further exacerbated when, in an apparent administrative error, the problem was instead misclassified as "low severity," allowing First American a full 90 days under its policies to remedy the breach. Still, following alleged "internal confusion and an alarming lack of accountability," the company failed to cure the defect even within that extended time frame, due in part to the assignment of the remedial efforts to a new employee who lacked data security experience.

After the vulnerability was publicized in May 2019, First American reported the breach to DFS and, following a forensic investigation of data exposure during an 11-month period beginning from June 2018, First American acknowledged that at least 350,000 documents were accessed without authorization by automated "bots" or "scrapers" that collect information available on the internet.

On July 22, 2020, DFS announced its enforcement action against First American,[2] charging the title insurer with violations of six separate provisions of its Cybersecurity Regulation.[3] Specifically, DFS charged first American with failing to:

- "maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability" of information systems that is "based on" a regulated entity's "risk assessment" and is aimed at "identifying and assessing internal and external cybersecurity risks that may threaten the security or integrity" of NPI, in violation of Section 500.02.[4] According to DFS, First American did not undertake any risk assessments of its FAST and EaglePro systems, despite the NPI stored and transmitted by those applications.
- "implement and maintain a written policy or policies" that would protect NPI transmitted by EaglePro, in violation of Section 500.03.[5] According to DFS, First American improperly classified EaglePro as an application that did not transmit NPI and "did not maintain an appropriate, risk-based policy governing access controls" for the application.
- "limit user access privileges" to NPI and to "periodically review such access privileges,"[6] in violation of Section 500.07, by allowing outside parties to obtain NPI documents merely by altering a URL.
- "conduct a periodic Risk Assessment" of its information systems that was "sufficient to inform the design of [its] cybersecurity program," in violation of Section 500.09.[7] According to DFS, this violation is evidenced by First American's failures to understand where NPI was stored in its systems and by its inability to protect NPI from unauthorized disclosure.
- provide its employees with "regular cybersecurity awareness training" that reflects its information security risks, in violation of Section 500.14(b).[8] According to DFS, First American did not provide adequate training to its title agents, who review and maintain documents containing NPI in the FAST and EaglePro systems, and upon whom First American relied to correctly identify and treat sensitive information.
- "implement controls, including encryption" of NPI that it stored and transmitted, in violation of Section 500.15, by failing to tag documents containing NPI and properly encrypt documents that it identified as containing NPI.[9]

Pursuant to its power under New York's Financial Services Law,[10] DFS's enforcement action seeks to impose on First American civil monetary penalties and an order requiring the company to remedy the asserted cybersecurity violations. In its press release announcing the enforcement action, DFS takes the position that "each instance" of NPI "encompassed by the charges" constitutes a separate infraction under the Regulations, "carrying up to $1,000 in penalties per violation."

IMPLICATIONS

These charges represent the first action by DFS to enforce its "first of its kind" cybersecurity Regulation intended to protect personal consumer information stored and transmitted by DFS-regulated financial institutions and insurance companies. Notably, in its charges, DFS focused on the asserted repeated failures of the company to remedy a known vulnerability, on the asserted delay in notifying DFS of the issue, and on an asserted lack of internal accountability that enabled repeated failures to occur, suggesting the particular importance of these issues to DFS.

This enforcement action may also signal DFS's intent to actively enforce the Regulations going forward. Regulated entities should review their compliance with the Regulations, and assess their systems and controls in light of the charges against First American. Among other things, regulated entities should have and implement robust internal policies governing the security of non-public consumer information they maintain, perform periodic assessments to verify that their policies are tailored to the particular risks that they face, and be mindful that relevant employees are regularly trained on how to identify and handle sensitive information and breaches. Moreover, regulated entities should have a comprehensive understanding of how NPI is received, stored, used or processed, and disseminated in the course of their business operations. Regulated entities should also take appropriate and prompt remedial action once they learn of a data breach, and should make clear the responsibilities of individual departments and employees in responding to vulnerabilities and data breaches. Failure to make adequate and timely notice of potential problems to regulators, or to promptly remediate vulnerabilities or act on a potential security breach, may result in liability under the Regulations. Notably, in the Statement of Charges, DFS focused on the fact that the cybersecurity vulnerabilities were only reported to DFS after first being publicized by a journalist.

The enforcement action against First American also sheds light on the magnitude of potential fines regulated entities may face for violations of the Regulations. As stated in its press release announcing these charges, DFS regards each instance of NPI exposure as a standalone violation of the Regulations, each of which could carry a penalty of up to a $1,000.[11] The allegations against First American, which involve tens of millions of exposed NPI documents, make clear that such an interpretation could in some cases enable DFS to impose very significant financial penalties under the Regulations.

* * *

ENDNOTES

1 Statement of Charges and Notice of Hearing, No. 2020-0030-C, *available at* https://www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf.

2 New York Department of Financial Services, 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), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221.

3 N.Y. COMP. CODES R. & REGS. tit. 23, § 500.0, *et seq.* *See* https://www.sullcrom.com/dfs-issues-updated-proposed-cybersecurity-regulations.

4 *Id.* § 500.2.

5 *Id.* § 500.3.

6 *Id.* § 500.7.

7 *Id.* § 500.9.

8 *Id.* § 500.14(b).

9 *Id.* § 500.15.

10 N.Y. FIN. SERV. LAW § 408.

11 *Id.* § 408(a)(2).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Robert G. DeLaMater	+1-212-558-4788	delamaterr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
C. Andrew Gerlach	+1-212-558-4789	gerlacha@sullcrom.com
Roderick M. Gilman Jr.	+1-212-558-3277	gilmanr@sullcrom.com
Stephen M. Kotran	+1-212-558-4963	kotrans@sullcrom.com
Marion Leydier	+1-212-558-7925	leydierm@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Sharon L. Nelles	+1-212-558-4976	nelless@sullcrom.com
Mark F. Rosenberg	+1-212-558-3647	rosenbergm@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
William D. Torchiana	+1-212-558-4056	torchianaw@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Julia M. Jordan	+1-202-956-7535	jordanjm@sullcrom.com
Kamil R. Shields	+1-202-956-7040	shieldsk@sullcrom.com

Los Angeles		
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com
Robert A. Sacks	+1-310-712-6640	sacksr@sullcrom.com
Palo Alto		
Scott D. Miller	+1-650-461-5620	millersc@sullcrom.com
Nadar A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Sarah P. Payne	+1-650-461-5669	paynesa@sullcrom.com
Paris		
William D. Torchiana	+33-1-7304-5890	torchianaw@sullcrom.com