DFS'S FIRST ENFORCEMENT ACTION PURSUANT TO ITS CYBERSECURITY REGULATION

Hodgson Russ Cybersecurity & Privacy Alert
August 5, 2020

Despite the fanfare of the DFS Regulation's debut, there has been little evidence of DFS enforcement — until now. Over three years ago, on March 1, 2017, the NY Department of Financial Services (DFS) issued its Cybersecurity Regulation (23 NYCRR 500). The DFS regulations apply to any person or entity that is required to operate with a license or registration under New York Banking Law, Insurance Law or the Financial Services Law. These so-called "Covered Entities" include, among other entities, banks, insurance companies and other financial service institutions. As the name suggests, the DFS regulations require Covered Entities to address the ever-growing threat posed to financial systems by cyber criminals, and to protect customers' nonpublic personal information ("NPI"). Among other things, Covered Entities must conduct regular security risk assessments, keep audit trails of asset use, provide defensive infrastructures, maintain policies and procedures for cyber security, create an incident response plan and manage third party vendors.

On Wednesday, July 22nd, DFS filed a twenty-one page Statement of Charges and Notice of Hearing against First American Title Insurance Company ("First American"), the second largest provider of title insurance in the United States. The Statement of Charges filed by DFS alleges that First American exposed hundreds of millions of documents, many of which contained customers' NPI, including bank account numbers, mortgage and tax records, Social Security Numbers, wire transaction receipts and drivers' license images. The enforcement action arises out of First American's use of EaglePro — a web-based title document delivery application. The application developed a vulnerability in October 2014 when the software was updated. As a result of the vulnerability, documents containing NPI were accessible from October 2014 until May 2019. First American's Cyber Defense Team discovered the vulnerability in December 2018 during a penetration test of the EaglePro application, but did not correct the problem for six months.

A number of deficient practices are alleged to have caused First American's failure to promptly detect and then remediate the vulnerability. Those deficiencies are reflected in the charges brought by DFS, as set forth below:

1. First American failed to perform risk assessments for data stored and transmitted within its Information Systems in violation of 23 NYCRR 500.02;

Attorneys

Jane Bello Burke
William Ciszewski III
Alfonzo Cutaia
Reetuparna Dutta
Patrick Fitzsimmons
Michael Flanagan
Michelle Merola
R. Kent Roberts
Gary Schober
Amy Walters

Practices & Industries

Cybersecurity & Privacy

2. First America failed to maintain and implement data governance and classification policies for NPI suitable to address the associated risks in violation of 23 NYCRR 500.03;
3. First American failed to limit user access privileges to Information Systems that provide access to NPI and to periodically review such access privileges in violation of 23 NYCRR 500.07;
4. First American failed to conduct a risk assessment sufficient to inform the design of the cybersecurity program, including identification of where NPI was stored and implementation of controls to protect it in violation of 23 NYCRR 500.09.
5. First American did not provide adequate data security training for its employees and affiliated title agents responsible for identifying and uploading NPI in violation of 23 NYCRR 500.14.
6. First American failed to encrypt documents marked as sensitive within their internal document repository, or otherwise implement controls suitable to protect NPI in violation of 23 NYCRR 500.15.

As a result of the Statement of Charges, First American faces a penalty of up to $1,000 per instance of exposed NPI. A hearing is scheduled for October 26, 2020 at which First American will answer to these charges. The enforcement hearing is expected to provide the public with a better understanding of both the enforcement priorities and future penalties associated with insufficient cybersecurity practices.

Although the DFS enforcement action against First American is the first, it is certainly not the last. And it is an important reminder that the DFS regulations do have teeth, requiring Covered Entities to reassess their security compliance lest they become the next target of DFS enforcement. Contact Michelle Merola (518.736.2917), Gary Schober (716.848.1289) or Patrick Fitzsimmons (716.848.1710) to discuss how Hodgson Russ LLP can assist you with compliance related to DFS's Cybersecurity Regulation.

If you received this alert from a third party or from visiting our website, and would like to be added to our Cybersecurity & Privacy alert mailing list or any other of our mailing lists, please visit us **HERE**.