NY Department of Financial Services Announces First Enforcement Action Under Cybersecurity Regulation

Alysa Z. Hutnik

July 24, 2020

On July 22, the New York Department of Financial Services (DFS) announced the first enforcement action under its new Cybersecurity Regulation, which requires that businesses registered or licensed by DFS comply with a number of robust cybersecurity requirements. The action involves First American Title Insurance Company and, according to the Statement of Charges and Notice of Hearing, a "known vulnerability" that exposed tens of millions of documents containing non-public personal information (NPI). First American maintained a document-sharing application, and a vulnerability within the application allowed anyone with the URL to access the document and the NPI contained therein. After the First American cybersecurity team discovered the vulnerability in December 2018 (four-and-a-half years after it first occurred), it classified the risk as "medium severity" and failed to take reasonable remedial steps.

DFS alleges these actions (or lack thereof) violated the following six requirements of the Cybersecurity Regulation:

1. Cybersecurity Program – The requirement to maintain a cybersecurity program that is designed to protect the confidentiality, integrity, and availability of information systems and to perform core cybersecurity functions, and that is based on a risk assessment.

2. Data Governance – The requirement to maintain and implement data governance and classification policies suitable to the business model and associated risks.

3. Access Privileges – The requirement to limit and periodically review user access privileges.

4. Risk Assessment – The requirement to conduct a periodic risk assessment that is sufficient to inform the design of the cybersecurity program.

5. Training – The requirement to provide regular cybersecurity awareness training for all personnel, and to update such training to reflect the risks identified in the risk assessment.

6. Controls – The requirement to implement controls, including encryption, to protect NPI held or transmitted.

DFS can assess up to $1,000 per violation, and has stated that it considers each instance of exposed NPI a separate violation. At the hearing, scheduled for October 26, 2020, DFS will determine whether violations have occurred. This enforcement proceeding is a good reminder of the importance of conducting periodic assessments of cybersecurity practices, and not simply going through the

motions of checking the boxes and filing the annual certification.

Summer associate Katrina Hatahet contributed to this post. Ms. Hatahet is not a practicing attorney and is practicing under the supervision of principals of the firm who are members of the D.C. Bar.