HINSHAW

Alerts

Cybersecurity Compliance Emphasized at MBA's Legal Issues and Regulatory Compliance Conference

June 3, 2021
Hinshaw Privacy & Cyber Bytes

With cybersecurity legislation and regulation sweeping the country in response to a series of high-profile hacking and ransomware attacks, it was little surprise that cybersecurity was a topic at the recently concluded Mortgage Bankers Association's Conference on Legal Issues and Regulatory Compliance. A major takeaway at the conference was that lenders and servicers with consumer-facing platforms that collect personal information should review their cybersecurity policies immediately. Simply waiting for an agency inquiry, investigation, or a breach could result in dire financial and reputational consequences.

To illustrate this point, one speaker at the conference noted the enforcement action commenced by the New York State Department of Financial Services (DFS) in July of 2020 against a leading title insurance company, alleging violations of DFS's Cybersecurity Regulation 23 NYCRR 500 (Regulation 500). Among other things, Regulation 500 requires that most financial institutions and other regulated businesses operating in New York have a robust written cybersecurity program informed by periodic risk assessments. The program should also include a plan to respond to and recover from cybersecurity incidents and trained cybersecurity personnel. Covered entities are further required to submit a certificate of compliance to DFS. Failure to adhere to the mandates of Regulation 500 subjects violators to penalties of $1,000 per incident.

DFS alleged that the insurer failed to follow its own cybersecurity policy after a vulnerability in its system exposed millions of files containing consumers' personal information, including bank account and social security numbers. DFS further alleged that the insurer misclassified the vulnerability as "low" in severity; failed to conduct a reasonable investigation into the scope and cause of the exposure; failed to utilize cybersecurity personnel; and falsely certified its compliance with Regulation 500. A hearing is scheduled for August of this year.

All businesses that collect the personal data of consumers should take heed of this enforcement action and adopt the following best practices:

- Follow written cybersecurity programs;
- Conduct regular risk assessments to detect vulnerabilities and update cybersecurity programs accordingly;

Attorneys

Jason J. Oliveri

Service Areas

Consumer Financial Services

Privacy, Security & Artificial Intelligence

Regulatory and Compliance Counseling

- Do not underestimate the level of risk associated with a vulnerability;
- Train and utilize cybersecurity personnel; and
- Adhere to representations concerning cybersecurity programs.

If you are unsure if your organization is in compliance with cybersecurity laws like Regulation 500, you should contact a trained legal professional for an assessment as soon as possible. Other than DFS and the Federal Trade Commission, agencies such as the Consumer Financial Protection Bureau and the Securities & Exchange Commission have shown an increased appetite for regulating and enforcing digital practices and risks. Now is the time to ensure that your organization is in compliance.