HINSHAW

# Long-Awaited DFS Cyber Enforcement Action Sees Charges Filed Against Title Insurer For Exposing Millions of Documents Containing Consumer Personal Information

**3 min read**
Jul 23, 2020

After several years of anticipation, the New York State Department of Financial Services (DFS) has filed its first enforcement action under the agency's groundbreaking and first-in-the-nation 2017 cybersecurity regulation (Part 500 of Title 23 of the New York Codes, Rules, and Regulations), which prescribes how financial services companies licensed to operate in New York should construct their cybersecurity programs. This action is a wakeup call to covered entities to fully implement the directives of Part 500.

A statement of charges was announced on July 21, 2020 against a large real estate title insurer alleging that a design defect in a data management computer program resulted in the exposure over the course of several years of hundreds of millions of documents—millions of which contained sensitive personal information of consumers, including bank account information, mortgage and tax records, Social Security Numbers, wire transaction receipts, and drivers' license images.

According to the charges, the company discovered the vulnerability and exposure as a result of penetration testing it conducted in 2018, but then failed on multiple levels to remedy the exposure promptly allowing the vulnerability and data exposure to persist from at least October 2014 through May 2019, including months after it was discovered. The company's primary regulator, the Nebraska Department of Insurance, examined the company's information security program and its response to the breach and said that the company appeared to

have adequate technology controls in place and that it was in compliance with the New York cybersecurity regulations as of June 30, 2019.

DFS alleges multiple failures—a so-called "cascade of errors"—including:

- failing to follow its own policies, neglecting to conduct a security review and risk assessment of the flawed computer program and the sensitive data associated with the data vulnerability;
- misclassifying the vulnerability as "low" severity despite the magnitude of the document exposure, while also failing to investigate the vulnerability within the time frame dictated by its own internal cybersecurity policies;
- after discovering the data exposure, failing to conduct a reasonable investigation into the scope and cause of the data exposure, reviewing only 10 of the millions of documents exposed and thereby grossly underestimating the seriousness of the vulnerability; and
- failing to follow the recommendations of its internal cybersecurity team to conduct further investigation into the vulnerability.

The charges detail how the company refused to implement practices recommended by its security team, including limiting access to sensitive applications to authenticated users and adding specified technical controls. Moreover, despite awareness of inadequate security controls, the company failed to implement centralized and coordinated employee training, and the company's Chief Information Security Officer told DFS that implementation of controls to protect nonpublic information (NPI) were not the responsibility of the information security department. Further, the Company assigned an employee with little experience in data security to remediate the vulnerability, and then compounded the situation by failing to provide that "unqualified" employee with adequate information and support.

DFS alleges the company violated six provisions of Part 500 (500.02 (to perform risk assessments for data stored or transmitted within its information systems); 500.03 (to maintain and implement data governance and classification policies for NPI suitable to its business model and associated risks and to maintain appropriate risk-based access controls policy); 500.07 (reasonable access controls); 500.09 (risk assessment sufficient to inform design of cyber program as required); 500.14 (to provide adequate data security training); and 500.15 (to encrypt documents containing NPI). A hearing on the charges will be held October 26, 2020. Each instance of nonpublic information constitutes a separate violation under applicable financial services law carrying up to $1,000 in penalties per violation. A full copy of the statement of charges and Notice of Hearing can be found on the Hinshaw website.

# Takeaway Thoughts

This first DFS enforcement action should serve as a wakeup call to covered entities that have not fully implemented the requirements of the cybersecurity regulation. Moreover, since DFS will be reviewing in substance the reasonableness and decision-making process supporting companies' actions taken with respect to

cybersecurity, companies should carefully document—and be prepared to defend—the rationale and governance process behind their actions.

---

*Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.*

## Topics

**New York, DFS, Cybersecurity, Regulatory, Regulatory Compliance, Part 500**

## Related Capabilities

Consumer Financial Services