Takeaways From NY's First Cybersecurity Enforcement Action

By **William Ridgway and Peter Cheun** (August 4, 2020)

William Ridgway

Peter Cheun

The New York State Department of Financial Services, or DFS, has filed its first charges against a financial institution for violating its cybersecurity regulation, signaling the need for covered entities to be mindful of their cybersecurity obligations.

On July 22, the DFS brought its first action under its groundbreaking cybersecurity regulations, delivering on the regulator's promise to prioritize enforcement. The DFS alleges that First American Title Insurance Co., the second-largest real estate title insurer in the U.S., exposed the personal and financial information of millions of consumers due to a website vulnerability that First American had known about from a routine penetration test required under the DFS cybersecurity regulations.

The vulnerability, which allegedly went undetected for years, created a flaw in the company's web-based document delivery system, enabling anyone to view up to 850 million documents, including many that contained sensitive nonpublic information, without needing a password.

This action comes about a year after the DFS established its cybersecurity division, which the agency described as the "first of its kind at a banking or insurance regulator," and appointed a former cybercrime prosecutor to serve as its leader. Against that backdrop, covered DFS-regulated banks, insurance companies and other financial institutions should expect future enforcement.

The Cybersecurity Regulations

New York's cybersecurity regulations, the first of their kind at the state level, require covered entities to establish and maintain cybersecurity programs designed to protect consumers and the financial services industry from the threat of cyberattacks. Announced in 2017, the regime's various provisions were phased into effect over the course of two years, with all requirements becoming fully effective by March 2019. Key requirements include:

- Written cybersecurity policies and procedures to protect information systems and the nonpublic information on those systems, including information systems and nonpublic information accessible to, or held by, third-party service providers;

- A written cybersecurity event response plan, including a 72-hour notification requirement;

- Periodic risk assessments, an annual penetration test and a biannual vulnerability assessment;

- Data retention policies and controls, including encryption, to protect nonpublic information, including for information held by third-party service providers;

- Regular cybersecurity awareness training for all personnel;

- Submission of the chief information security officer's report on the company's cybersecurity program to the board or a senior officer; and

- An annual written statement to the DFS certifying that the entity is in compliance with the cybersecurity regulations.

Takeaways

As these regulations have come into force, the DFS warned that failure to comply with the requirements may lead to enforcement, a threat the regulator followed through on with its statement of action against First American. The details from that statement provide insights into both the priorities and expectations of the DFS and the manner in which other regulators may interpret similar data security laws that have been adopted by states across the U.S.

Organizations should consider the following in light of the First American case.

Remediate Identified Vulnerabilities Promptly

The DFS' action highlights how the mandate to conduct periodic penetration testing and vulnerability assessments can expose covered entities to enforcement risk. These tests are standard in most sectors and routinely uncover vulnerabilities, even at organizations with robust security programs.

Most organizations have a policy for remediating the identified vulnerabilities within a time frame in accordance with their severity. These remediation processes will now take on heightened significance after the DFS codified these best practices into a regulatory mandate, as the First American action reveals.

The DFS complaint alleges that First American identified the vulnerability at issue pursuant to a mandated penetration test but underestimated the risk it posed, leading the company to conclude that it had 90 days to remediate under its policies. The DFS also criticized the company for assigning "a new employee with little experience in data security" to remediate the vulnerability and for reviewing only 10 out of the potentially hundreds of millions of documents exposed, which the DFS characterized as "unacceptably minimal."

In-house cybersecurity experts at the company also advised further review of the vulnerability, the DFS claims, but nothing came of that recommendation. Finally, the DFS detailed the company's noncompliance with its own remediation policies, including its failure to remediate within 90 days and appropriately follow up on the risk assessment.

These allegations underscore the need for companies to remediate vulnerabilities identified during penetration tests and vulnerability assessments in a timely manner with capable personnel, and to document those efforts in contemporaneous records. A failure to follow through on those processes may be judged harshly by an enforcement agency.

Perform and Document Risk Assessments

The state's cybersecurity regulations require a periodic risk assessment of information systems, and the statement of action reveals that the DFS may scrutinize the scope and depth of those assessments, including which particular systems were reviewed.

In its statement, the DFS highlighted the lack of a documented risk assessment of the document delivery system at issue as a key failure for First American, in addition to its failure to identify that the system contained nonpublic information, and to identify the availability and effectiveness of controls to protect that information. Thus, covered entities should consider taking proactive measures to identify each information system involving nonpublic information, and perform and document appropriate risk assessments.

Provide Cybersecurity Awareness Training for Key Personnel

A regulatory inquiry from the DFS following an incident may include questions about cybersecurity awareness training, which is required by the regulations. The DFS deemed First American's training to be inadequate because the company allegedly delegated the effort to individual business units to design training at their own discretion without any centralization or coordination.

That failure, the DFS asserts, was compounded by the fact that the company's sole control to prevent the storage and transmission of sensitive information on the document delivery system was an employee policy against doing so. In view of these allegations, covered entities should coordinate and vet their cybersecurity training programs while also paying special attention to employees who handle and control access to sensitive information.

Beware of Potential Penalties, Even Without Alleged Harm to Consumers

Although the cybersecurity regulations do not provide for penalties, they empower the DFS to pursue enforcement under any applicable laws. In announcing the action against First American, the DFS invoked Section 408 of the New York Financial Services Law and claimed penalties of up to $1,000 for "each instance of nonpublic information encompassed within the charges," a potentially substantial liability for an incident that may involve hundreds of millions of consumer records.[1]

Notably absent from the DFS' statement was an allegation of direct consumer harm arising from the exposure — a key detail that often influences the amount of financial exposure a company faces in the wake of an incident. Given that data breaches routinely involve the exposure of millions of records, the DFS' position on enforcement raises the specter of staggering penalties even without identifiable harm to consumers.

Conclusion

Although it remains unclear how frequently the DFS will resort to enforcement actions, the case against First American provides important clues. Covered entities that suffer an incident should expect their policies, procedures and practices to come under close scrutiny.

The risk of significant financial penalties provides even more reason for covered entities to reassess their compliance with the cybersecurity regulations before an attack strikes.

William Ridgway is a partner and Peter Cheun is an associate at Skadden Arps Slate Meagher & Flom LLP.

[1] DFS Press Release, July 22, 2020, outlining the charges. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221