Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

NY Cybersecurity Rules Pack Wallop In Enforcement Debut

By **Allison Grande**

Law360 (August 18, 2020, 8:36 PM EDT) -- New York's financial services regulator demonstrated an appetite for policing data security missteps, even if consumers aren't obviously harmed, by targeting a data leak at insurer First American for its first enforcement action under the state's novel cybersecurity rules.

Banks and insurers have long been bracing for enforcement to begin under first-of-their-kind cybersecurity rules developed by the New York Department of Financial Services in 2016. The regulations, which require covered entities to take specific steps to fortify their cybersecurity protocols and to report breaches within 72 hours, took effect in several stages spanning a two-year period that concluded in March 2019.

With the rules now fully operational, the regulator on July 21 plunged into the enforcement arena by announcing charges against First American Title Insurance Co. stemming from an alleged vulnerability in the company's information systems that led to millions of consumers' sensitive personal information being exposed. The California-based insurer is contesting these allegations, and a hearing in the matter has been set for Oct. 26.

"With First American saying that it intends to defend itself against the regulator's statement of charges, that means that a full record will likely be developed and there will be an opportunity for the entire industry to get more clarity about the extent of the department's authority and the expansiveness of the regulation," said Jonno Forman, a New-York based partner at BakerHostetler.

A major point of contention between the insurer and regulator will likely be "over the difference between the possibility that data was exposed versus whether data actually was exposed and, if so, whether any harm flowed to the individuals," according to Jena Valdetero, co-head of the data privacy and security team at Bryan Cave Leighton Paisner LLP.

"The answer to that question should have a large impact on the amount of any fine or settlement," Valdetero said.

That fight is also poised to have significant ramifications for other insurers and financial institutions regulated by the department, according to attorneys.

The regulator is arguing that First American violated six provisions of the landmark cybersecurity regulations in its handling of a breach that resulted in an estimated 885 million mortgage records being available to "anyone with a web browser" from at least October 2014 through May 2019. The statement of

charges asserts that First American knew about the vulnerability on its public-facing website that led to the exposure but didn't act appropriately to fix the flaw.

The regulator has asserted that each exposed record counts as a separate violation for which it has the power to recover $1,000.

First American has countered that its own investigation has revealed that only a "very limited number" of consumers — and none from New York — had personal information exposed.

Unlike private litigation, where plaintiffs need to allege a concrete injury in order to establish the Article III standing necessary to move forward with their claims, the financial services authority only needs to assert a violation of the cybersecurity regulations, rather than allege actual harm, to bring an enforcement action. By electing to come out of the gate with an action where there's no clear consumer harm, the regulator has solidified an aggressive stance toward noncompliance that threatens to sweep up a wide range of misconduct, attorneys say.

"The breadth of the DFS' authority over cybersecurity events that do not have direct harm on New York consumers is something that we'll likely get clarity on, and that will be significant," Forman said.

Andrew Jacobson, a New York-based attorney at Seward & Kissel LLP and a former enforcement attorney at DFS, noted that most of the regulator's enforcement actions are resolved by consent order and that it's fairly rare for the department to bring charges via an administrative hearing, signaling that the issues at the heart of the First American case are "clearly a priority for the agency."

"DFS's charges, in this case, represent not only its first enforcement action under the cybersecurity regulation, but DFS's continued efforts to hold regulated entities accountable," Jacobson said.

When DFS moved nearly four years ago to significantly raise the cybersecurity compliance bar for financial institutions, there was little doubt that the agency would be aggressive in ensuring that companies were complying with their new technical and reporting obligations.

At least publicly, the regulator's oversight in this area to date has appeared to focus primarily on educating covered entities about the regulations and assisting them with compliance. But last month's action shows that the department is ready and willing to activate its enforcement powers when necessary to address conduct that it finds to be particularly troubling, according to attorneys.

"DFS is clearly focused on holding regulated entities accountable, and in this particular situation, the alleged willfulness of the conduct appears to have added to the seriousness of the charges," Jacobson added.

In laying out its charges against First American, the regulator has sent several important signals about its cybersecurity expectations and how it's planning to enforce its rules moving forward, according to attorneys.

"Companies need to take a look at the statement of charges and look at their own programs, and then think long and hard if they're a licensed entity covered by DFS about whether their cybersecurity policies are just window dressings or if they really mean something," said Cynthia Larose, chair of Mintz Levin Cohn Ferris Glovsky and Popeo PC's privacy practice.

The cybersecurity rules require covered entities to set out detailed plans for handling vulnerabilities and data breaches; increase their monitoring of how third-party vendors handle and secure customer data; and appoint a chief information security officer, among other requirements.

In its first foray into enforcement, the department took particular aim at First American's penetration testing and risk assessment procedures.

Specifically, the department said First American failed to follow its own policies and neglected to conduct a security review and risk assessment of the flawed computer program. The insurer also misclassified the vulnerability as "low" in severity despite the sheer magnitude of the document exposure, according to the regulator. And it failed to investigate the vulnerability within the time frame dictated by its internal cybersecurity policies, the department said.

The Department of Financial Services added that after the exposure was discovered by an internal test in December 2018, First American didn't conduct a "reasonable investigation" into the scope and cause of the exposure and reviewed only 10 of the millions of documents exposed.

"The department's first enforcement action highlights that it will not consider it to be sufficient for a covered entity to simply conduct a security risk assessment alone — the risks identified by the assessment must be quickly remediated." Bryan Cave's Valdetero said.

Financial institutions would be wise to pay heed to this lesson, given that this misstep isn't uncommon.

"Many companies struggle to close the gaps revealed by a risk assessment, and the department's first enforcement action makes clear that there will be a regulatory price to pay for not doing so," Valdetero said.

Phillips Nizer LLP technology practice chair Thomas Jackson agreed that the First American action demonstrates the importance of not only conducting "comprehensive risk assessments by qualified experts and knowledgeable, well-trained staff" but also of being able to implement effective access control measures, develop effective data governance and classification policies, and ensure that vulnerabilities are remedied once they're detected.

"All [are] critical elements of a well-thought through cybersecurity program," Jackson said.

The regulator's focus on the timing and manner of the insurer's response to the vulnerability once it was identified is also notable, according to Mark Krotoski, co-head of privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

"This is part of a recent trend among other enforcers focused on timeliness," he said.

For companies that experience a data security incident that they're required to report to DFS, heeding these lessons and ensuring that robust measures are in place will be vital for when the regulator comes knocking, attorneys say.

"Breaches happen even to companies with the best security," Larose said. "But if you're on top of it and do all of the steps required under the regulation, it seems unlikely that DFS is going to spend its time bringing an enforcement action."

Being aware of the department's expectations is also likely to be beneficial to financial institutions even if they don't have a breach, given that the regulator is empowered to look for cybersecurity deficiencies during its regular examination activities and bring enforcement actions if it finds that these procedures aren't up to par, attorneys added.

Krotoski noted that the vulnerability at the center of the First American action appeared to have been identified through a penetration test, which is one of the specific forms of testing mandated by the cybersecurity regulation.

Given this development, chances are high that the regulator will move to use records that companies are required to maintain and disclose under the regulation, including the results of penetration tests and their annual reports certifying they're in compliance with the rules, against them in enforcement proceedings, attorneys noted.

While the regulator and First American may reach a deal to resolve the dispute before the October hearing, if the case proceeds to this phase, the insurer is likely to face an uphill battle in contesting the claims against it, according to Jacobson, the former DFS enforcement attorney.

"It is not clear yet what First American's defenses will be, but it is extraordinarily difficult for companies to win in an administrative hearing against DFS," he said, adding that "the consequences of such a hearing can be tremendous, including monetary penalties, reputational harm, and revocation of the entity's operating license."

Regardless of how the First American action plays out, attorneys agree that it's a strong opening salvo for the financial services regulator, as well as a good indicator of what's to come.

DFS is widely expected to remain active in this space, especially in light of Superintendent Linda A. Lacewell last year moving to create a dedicated cybersecurity division. The unit is the first of its kind for a financial industry regulator and stands on equal footing with the regulator's banking, insurance and consumer protection and financial enforcement divisions.

"DFS' statement of charges against First American signals a shift in its enforcement policy toward a greater emphasis on consumer protection and likely indicates that the agency plans to enforce its cybersecurity regulations more actively in the future," Jackson, of Phillips Nizer, said.

The New York State Department of Financial Services is represented by Katherine A. Lemire, Desiree S. Murnane, Elizabeth Farid and Madeline W. Murphy of the Consumer Protection and Financial Enforcement Division, and Justin S. Herring of the Cybersecurity Division.

Counsel information for First American wasn't immediately available.

The case is In the Matter of First American Title Insurance Co., case number 2020-0030-C, in the New York State Department of Financial Services.

--Additional reporting by Hailey Konnath. Editing by Emily Kokoll and Orlando Lorenzo.