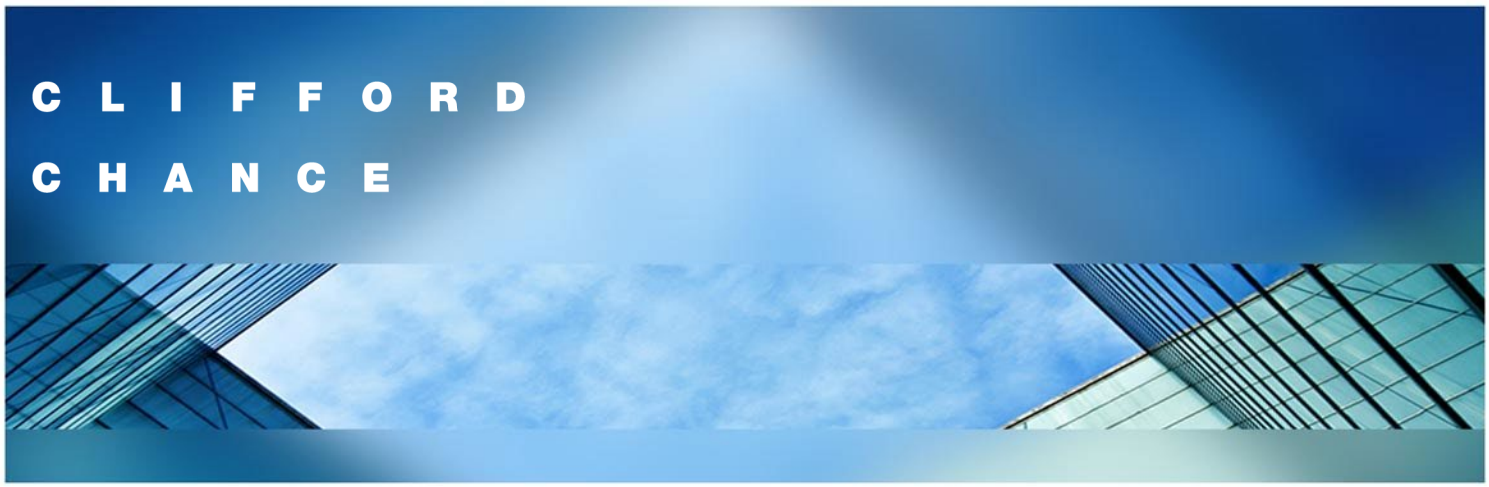

NYDFS ANNOUNCES FIRST ENFORCEMENT ACTION UNDER CYBERSECURITY REGULATION

On Wednesday, July 22, the New York Department of Financial Services ("NYDFS") charged First American Title Insurance Company with multiple violations of NYDFS's Cybersecurity Regulation, 23 NYCRR 500. This is the Department's first enforcement action since the Regulation took effect on March 1, 2017, signalling that the Regulation definitely has teeth and carries the prospect of severe penalties for those who have not yet taken it seriously. The action thus provides important guidance to NYDFS-supervised entities, particularly given the heightened risk of cybersecurity incidents during the COVID-19 pandemic.

OVERVIEW OF NYDFS AND THE CYBERSECURITY REGULATION

NYDFS issued the Cybersecurity Regulation in 2017, the first set of comprehensive cybersecurity rules issued by a state banking or insurance regulator. The Regulation requires entities supervised by the Department to have in place a "robust" cybersecurity program designed to protect the confidentiality, integrity and availability of its information systems. The rules require covered entities to identify and address vulnerabilities identified through regular risk assessments and implement certain controls and policies such as user access controls, encryption, multi-factor authentication, incident response, policies to address risks from third-party service providers, and regular cybersecurity awareness training for employees. Covered entities are also required to notify NYDFS within 72 hours of identifying a cybersecurity incident and to make annual certifications to the Superintendent regarding compliance with the Regulation.[1]

THE ENFORCEMENT ACTION

NYDFS's enforcement notice alleges that from October 2014 through May 2019, a vulnerability in First American's website allowed public access to hundreds of

[1] For a discussion of the Regulation and its requirements, see our briefing here.

millions of documents containing sensitive personal information of consumers, including bank account numbers, financial records, Social Security numbers, and drivers' license images. According to the complaint, First American's Cyber Defense Team identified the vulnerability in December of 2018 during a routine penetration test, but the company did not take steps to remediate the exposure until May 2019, when a journalist published a news article documenting the vulnerability. A subsequent investigation determined that at least 350,000 documents were accessed without authorization.

According to NYDFS, the delay in remediation was due to First American's ineffective incident response policies, as well as failure to follow even those policies. These issues include:

- **Failure to properly investigate the identified vulnerability**. After First American's Cyber Defense Team determined that internal documents were exposed, it reviewed a sample of ten documents to determine whether sensitive personal information was included—a "preposterously minimal review" according to the complaint. No further investigation was conducted despite the Team's recommendation to do additional review.
- **Failure to adhere to internal policies**. First American initially classified the vulnerability as "medium" risk before accidentally re-classifying the risk as "low" severity. Nevertheless, its internal policies required the company to remediate "low" risks within 90 days (which it did not).
- **Insufficient resources dedicated to cybersecurity**. First American assigned responsibility for remediation of the vulnerability to an employee who was new to the company, had little experience in data security, and was not given relevant information about the vulnerability (including the report on the penetration test identifying the vulnerability).
- **Improper controls to protect sensitive information**. First American relied on employees to tag documents that contained personal information, a manual process that the company had determined internally to be "highly prone to error" with an error rate as high as 30%. After the news report exposed the vulnerability, First American's cybersecurity team recommended that the company implement access controls and technical controls—all of which senior management rejected. Instead, the company delegated responsibility to employees to avoid using the compromised system to transmit documents that contain personal information.
- **Lack of accountability**. NYDFS's complaint states that after interviewing First American employees, it identified an "alarming lack of accountability" over cybersecurity controls. According to NYDFS, when it asked First American's CISO about the company's lack of controls, the CISO "disavowed" ownership of the issue, stating that this was the responsibility of other departments.

NYDFS alleges that these failures amount to violations of its Cybersecurity Regulation, and accordingly it has issued a charging notice seeking civil monetary penalties as well as an injunction requiring First American to remediate the violations.

CONCLUSION: WHAT TO WATCH

Practitioners and covered entities have been anticipating an enforcement action for some time now. Even though the Regulations were issued in March 2017, they did not become fully effective until March of 2019, following a two-year phased implementation process. Shortly afterwards, NYDFS established a Cybersecurity Division to focus on enforcing the Regulation and combatting cybercrime.

This action—filed by the Cybersecurity Division—signals that NYDFS is ready to begin actively enforcing the Cybersecurity Regulation. This comes at an interesting time, given the heightened cyber risks NYDFS has identified in the current pandemic environment.[2] Now more than ever it is important for companies—particularly those supervised by NYDFS—to have effective cybersecurity policies and procedures in place to defend against unauthorized access and disruption.

The First American action is scheduled for a hearing before NYDFS beginning on October 26, 2020.

[2] For a discussion of recent guidance from NYDFS regarding heightened cybersecurity risks in today's "WFH" environment, see our briefing here.

CONTACTS

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA