Simpson Thacher

Regulatory and Enforcement Alert

As Cyber Incidents Continue to Rise, the SEC Charges Issuer for Inadequate Disclosure Controls in the Context of a Data Breach

June 17, 2021

The SEC announced on June 15 that it settled administrative charges against First American Financial Corporation, a mortgage title and settlement services company, for failing to maintain adequate disclosure controls and procedures in connection with a 2019 cybersecurity breach.

According to the SEC's Order, in May 2019, a cybersecurity journalist informed First American of a breach that exposed more than 800 million images and included customers' sensitive personal data. Although First American promptly informed the SEC and filed a Form 8-K disclosing the incident, the Order found that the senior executives who were responsible for the company's public statements were not made aware of key information regarding the breach, including that First American's cybersecurity team had identified the vulnerability months earlier and had failed to fix the issue or report it up the ladder.

The SEC found that the company failed to maintain disclosure controls and procedures ensuring that relevant information regarding the breach was properly escalated and analyzed. An SEC official stated that "issuers must ensure that information important to investors is reported up the corporate ladder to those responsible for disclosures." First American agreed to pay a $487,616 penalty without admitting or denying the SEC's findings.

The settlement was announced shortly after the SEC indicated its plans to recommend rule amendments to "enhance issuer disclosures regarding cybersecurity risk governance," with a target release date of October 2021. Any such rule would underscore the message going back a number of years that the Commission is focused on cybersecurity disclosures and related controls. In 2018, Yahoo! paid a $35 million penalty to settle charges that it misled investors by failing to disclose a data breach. In 2018, the Commission issued a Section 21(a) report that directed issuers to consider cyber-related risks when devising and maintaining internal accounting controls. And also in 2018, the Commission released its Interpretative Guidance on Cybersecurity Disclosures, which stated in relevant part:

> "Crucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that such matters may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents. In addition, the Commission believes that the

development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face."

Given the Commission's continued focus on cybersecurity-related disclosures, and the controls and procedures surrounding such disclosures, public companies should further ensure that disclosure committees (or the equivalent teams charged with preparing public disclosures) have representation from all relevant parts of the organization to ensure all relevant information about potential cybersecurity issues is timely escalated and integrated into the disclosure process.

For further information about this Alert, please contact one of the following members of the Firm's Litigation Department.

NEW YORK CITY

Marc P. Berger
+1-212-455-2197
marc.berger@stblaw.com

Brooke E. Cucinella
+1-212-455-3070
brooke.cucinella@stblaw.com

Stephen M. Cutler
+1-212-455-2773
stephen.cutler@stblaw.com

Nicholas S. Goldin
+1-212-455-3685
ngoldin@stblaw.com

Michael J. Osnato, Jr.
+1-212-455-3252
michael.osnato@stblaw.com

SÃO PAULO

Rafael M. Loureiro
+55-11-3546-1026
rafael.loureiro@stblaw.com