Published on *The National Law Review* https://natlawreview.com

Ensure Disclosure Controls and Procedures Address Cybersecurity

Article By:

Peter D. Fetzer

Stuart E. Fross

Stephen M. Meli

Margaret Gembala Nelson

Thomas J. Krysa

On June 15, 2021, the Securities and Exchange Commission (SEC) announced settled charges against real estate settlement services company First American Financial Corporation for disclosure controls and procedures violations related to a cybersecurity vulnerability that exposed sensitive customer information. The SEC's order charges First American with violating Rule 13a-15(a) of the Securities Exchange Act of 1934. Without admitting or denying the SEC's findings, First American agreed to a cease-and-desist order and to pay a $487,616 penalty.

Why We are Sending this Alert: To remind issuers that they should ensure that their disclosure controls and procedures address cybersecurity and include elements intended to ensure that there is an analysis of potential disclosure obligations arising from cyberattacks and security breaches.

Details of SEC's Order: As reported by the SEC, on the morning of May 24, 2019, a cybersecurity journalist notified First American of a vulnerability with its application for sharing document images that exposed over 800 million images dating back to 2003, including images containing sensitive personal data such as social security numbers and financial information. In response, according to the order, First American issued a press statement on the evening of May 24, 2019, and furnished a Form 8-K to the Commission on May 28, 2019. However, according to the order, First American's senior executives responsible for these public statements were not apprised of certain information that was relevant to their assessment of the company's disclosure response to the vulnerability and the magnitude of the resulting risk.

The order finds that First American's senior executives were not informed that the company's information security personnel had identified the vulnerability several months earlier, but had failed to remediate it in accordance with the company's policies. The order finds that First American failed to

maintain disclosure controls and procedures designed to ensure that all available, relevant information concerning the vulnerability was analyzed for disclosure in the company's public reports filed with the Commission.

"As a result of First American's deficient disclosure controls, senior management was completely unaware of this vulnerability and the company's failure to remediate it," said Kristina Littman, Chief of the SEC Enforcement Division's Cyber Unit. She also stated, "Issuers must ensure that information important to investors is reported up the corporate ladder to those responsible for disclosures," and "First American did not have any disclosure controls and procedures related to cybersecurity, including incidents involving potential breaches of that data."

Action Items: The order is a reminder that issuers should ensure that their disclosure controls and procedures address cybersecurity and include elements intended to ensure that there is an analysis of potential disclosure obligations arising from cyberattacks and security breaches. At a minimum, disclosure controls and procedures and related protocols should specifically provide that cybersecurity incidents are promptly escalated and investigated, and reported to senior management, and where appropriate, to the Board of Directors.

Issuers should also consider reviewing their compliance programs to address the potential applicability of restrictions against trading while in possession of material, nonpublic information in connection with a cyberattack or security breach.

National Law Review, Volume XI, Number 167