BRACEWELL

INSIGHTS

SEC Gets Cyber-Serious About Disclosures

June 21, 2021

*By: **Matthew G. Nielsen** **Seth D. DuCharme***

As cyberattacks continue to attract greater attention, the SEC has taken an additional step in its efforts to bring enforcement actions related to cyber disclosures. On June 14, the SEC ***announced*** settled charges against a real estate settlement services company, First American Financial Corporation ("First American"), after determining that First American lacked sufficient internal controls, which caused the company to make an untimely, and thus improper, disclosure of a cybersecurity "vulnerability." Without admitting or denying the charges, First American agreed to a cease-and-desist order and to pay a $487,616 penalty.

According to the SEC's order, in May of 2019, a cybersecurity journalist informed First American that one of its software programs contained a substantial vulnerability. The vulnerability exposed over 800 million files of potentially sensitive data, such as social security numbers and financial information. After the journalist's tip, First American quickly released a ***statement*** and filed an update on Form 8-K to inform the SEC.

The SEC asserts, however, that the company's IT team identified the vulnerability months earlier and marked it as a "low risk" vulnerability in an internal report. The SEC also determined that First American's IT team failed to remediate the vulnerability as its policies required. Ultimately, there were no procedures in place wherein senior executives were apprised of the report or the vulnerability.

Over the past year, the SEC has levied multi-million dollar fines against a number of companies, including ***GE***, ***HP, Inc.***, and ***Morningstar***, for internal controls failures. The SEC's charges against First American are similar, but the ***order*** charging First American with violating Rule 13a-15(a) of the Securities Exchange Act for failing to maintain disclosure controls and procedures is the first time the SEC has brought these charges in connection with cybersecurity disclosures.

And unlike previous cyber-related SEC actions, there is neither evidence nor suggestion of a hack. Instead, the SEC brought charges because although First American's business involved handling data for real estate transactions, the company did not have "any disclosure controls and procedures related to cybersecurity, including incidents involving potential breaches of that data."

The SEC's new attention to cyber disclosure controls and procedures is one of many recent indicators that it expects companies to treat cyber hygiene as a material consideration for investors. "Issuers must ensure that information important to investors is reported up the corporate ladder to those responsible for disclosures," said Kristina Littman, Chief of the SEC Enforcement Division's Cyber Unit. "First American did not have any disclosure controls and procedures related to cybersecurity, including incidents involving potential breaches of that data."

While this is the first time the SEC has pursued an enforcement action for failures to maintain appropriate cyber disclosure controls, the SEC's concerns in this arena are not new. In 2018 ***guidance***, the second and most recent SEC guidance on cyber disclosure, the SEC explicitly encouraged companies to establish disclosure procedures for cyber risks and incidents:

"Controls and procedures should enable companies to identify cybersecurity risks and incidents, assess and analyze their impact on a company's business, evaluate the significance associated with such risks and incidents, provide for open communications between technical experts and disclosure advisors, and make timely disclosures regarding such risks and incidents."

System control failures have been a frequent point of general disclosure enforcement, and the SEC has already made it clear that cyber enforcement is a ***focus*** area for the new administration. But now, through disclosure control violations, cyber enforcement will reach not only data breaches and hacks that *have* impacted consumers, but also vulnerabilities that *could* impact consumers. This forward-looking approach reflects a new perspective on cyber-risk, and a perspective that is almost certain to evolve as rapidly as cyber risks themselves evolve.

The sensitivity and fluidity of cybersecurity has complicated SEC rulemaking in the cyber arena, but beyond pulling additional enforcement tools out of its toolbox, the SEC appears ***poised*** to update its guidance on cyber disclosure as ***early*** as October 2021. In the meantime, issuers should take enforcement actions like the one against First American seriously and reflect on whether their disclosure controls and procedures would have alerted senior management of a systems vulnerability like the one experienced by First American.

The cost—financial, reputational, and otherwise—of cyberattacks means that executives are more likely to hear about such events, even absent appropriate disclosure controls. But this SEC order is a reminder that where a company faces a cyber risk that does not necessarily incur those costs, it cannot be assumed that such risks will reach the right executives and, thus, be properly and timely disclosed.

Based on the First American order, it is reasonable to expect that the upcoming cyber guidance from the SEC will almost certainly emphasize disclosure controls for all types of cyber risk. Bracewell attorneys are ready to help companies navigate the changing landscape around cyber disclosures and SEC enforcement.