SULLIVAN & CROMWELL LLP

S&C memo

June 17, 2021

SEC Charges Issuer for Inadequate Cybersecurity Disclosure Controls

Action May Suggest a More Active SEC Enforcement Role Concerning Disclosure Controls and Procedures for Cybersecurity

SUMMARY

On June 15, 2021, the Securities and Exchange Commission ("SEC") announced charges against First American Financial Corporation ("First American") for failure to maintain adequate disclosure controls and procedures in violation of Exchange Act Rule 13a-15(a).[1] The charges, which were simultaneously settled pursuant to a cease-and-desist order (the "Order") imposing a $487,616 civil money penalty, related to a vulnerability in First American's proprietary software application that caused tens of millions of document images—many containing consumers' personal information—to be publicly accessible. After being notified by a journalist about the vulnerability on May 24, 2019, First American issued a press release and subsequently filed a Form 8-K with the SEC. According to the Order, however, the senior executives responsible for these disclosures were not informed prior to the time the disclosures were made that certain First American personnel had longstanding prior knowledge of the vulnerability, and that the vulnerability had not been remediated in accordance with the company's policies. In light of the action—and increased scrutiny by U.S. authorities concerning cybersecurity—issuers should review their disclosure controls and procedures for analyzing and escalating key information about cybersecurity incidents and vulnerabilities, and ensure that any response conforms with those policies.

BACKGROUND

As described by the Order,[2] First American issues title insurance and provides closing and escrow services. These services sometimes involved data with customers' non-public personal information ("NPPI"). As of May 24, 2019, First American stored documents containing such NPPI in a digital repository. Using a proprietary application called "EaglePro," First American employees could transmit images of documents

from the repository to customers. EaglePro provided recipients with a URL web link which, for "unsecure" EaglePro packages, permitted access to shared documents without password verification. According to the Order, First American employees were supposed to manually tag document containing NPPI with "SEC" (i.e., "secure"), but, based on an internal First American analysis from 2018, tens of millions of document images containing NPPI may have been stored in the repository without the "SEC" tag.

The Order states that, due to a defect introduced to EaglePro in 2014, a recipient of an EaglePro URL could view other repository documents—to which that user should not have access—simply by altering the digits of the URL corresponding to a document's numerical identifier, because according to the cybersecurity journalist, those identifiers may have been assigned sequentially. Further, certain document images sent through unsecure EaglePro packages were cached by public search engines.

The Order finds that although an internal cybersecurity test conducted between December 2018 and January 2019 alerted First American to this vulnerability, the company failed to comply with its vulnerability remediation management ("VRM") policies in addressing the issue. First American information security personnel finalized a report on the vulnerability on January 11, 2019 (the "January 2019 Report") describing the vulnerability and categorizing it as "level 3," or "medium risk," severity. In an apparent clerical error, the vulnerability was then erroneously inputted as "level 2," or "low risk" severity in First American's VRM tracking system, providing the company with 90 days rather than the required 45 days under its VRM policies to remedy the vulnerability. According to the Order, the company failed to cure the defect even within that extended 90-day time frame, and contrary to VRM policies, no waiver or risk acceptance was requested from the CISO.

The Order states that, after notifying First American about the vulnerability on May 24, 2019, a cybersecurity journalist published an article about it later that day. First American provided a statement to the journalist for inclusion in the article, and the same statement was disseminated to other news outlets. On May 28, 2019, First American filed a Form 8-K with the SEC. The Form 8-K attached a press release which asserted that there was "[n]o preliminary indication of large-scale unauthorized access to customer information."

According to the Order, neither the executives responsible for the aforementioned disclosures, nor the CISO and CIO, were timely made aware of the scale and history of the vulnerability, and even after the CISO and CIO learned of it, they did not disclose the information to executives responsible for disclosure decisions. Specifically, certain senior technical personnel, including the CISO and the CIO, only became aware of the January 2019 Report and the failure to remediate the vulnerability shortly after the journalist contacted First American on May 24, 2019. Thereafter, between May 24, 2019, and May 28, 2019, the "CISO and CIO participated in numerous meetings with the company's senior executives responsible for the company's disclosures," but failed to make the senior executives, including the CEO and CFO, aware of the January 2019 Report or the underlying vulnerability prior to the disclosures being made. Without this information, the executives making the disclosures "did not evaluate whether to disclose the company's prior awareness

of, or actions related to the vulnerability" and "lacked certain information to fully evaluate the company's cybersecurity responsiveness and the magnitude of the risk from the EaglePro vulnerability at the time they approved the company's disclosures."

The Order focuses in particular on (1) the fact that, once alerted by the journalist to the vulnerability, senior management was not made aware of all relevant information necessary to make a complete and accurate disclosure assessment, (2) the company's lack of *any* disclosure controls and procedures related to cybersecurity (particularly in light of the SEC's 2018 guidance in this area) and (3) the company's failure to follow its own policies for remediating cybersecurity vulnerability incidents.

The Order charges a violation of Rule 13a-15(a) of the Exchange Act, which requires that covered issuers maintain disclosure controls and procedures "that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the Act . . . is recorded, processed, summarized and reported, within the time periods specified" by the SEC.[3] These controls and procedures must ensure that information required to be disclosed is communicated to senior management.[4]

Without admitting or denying the SEC's findings, First American submitted an Offer of Settlement and agreed to pay a civil penalty of $487,616 and to cease and desist any violations of Rule 13a-15.[5]

The matter is also the subject of a New York State Department of Financial Services ("DFS") enforcement action brought against First American on July 22, 2020—the first enforcement action brought by the DFS under its cybersecurity regulations, 23 NYCRR Part 500.[6] A hearing in the DFS action is currently scheduled for August 16, 2021.[7]

IMPLICATIONS

This is only the second enforcement action the SEC has brought that is focused on disclosure controls and procedures for cybersecurity since the SEC issued interpretative guidance on the subject, and a related enforcement action, in 2018.[8] The fact that the SEC has brought a second action in this area after a period of three years may indicate that the SEC is particularly focused on timely disclosure of cybersecurity risks and incidents at a time when companies across industries in the United States are experiencing an onslaught of cyberattacks, from systemic supply-chain compromises to ransomware attacks and cyber-extortion schemes.

The SEC action coincides with heightened focus across the federal government on cybersecurity and information-sharing about cyberattacks. Among other things, President Biden recently issued an Executive Order on Improving the Nation's Cybersecurity, which mandates increased information-sharing on cyber incidents for certain government service providers, among other requirements.[9] In addition, the Biden Administration recently issued an open memorandum to "Corporate Executives and Business Leaders," which called on U.S. business executives, in light of the escalation in ransomware attacks, to "immediately

convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans."[10]

Given the SEC's—as well as other U.S. regulators'—heightened focus on cybersecurity, issuers should review their policies and disclosure controls and procedures to assess whether they provide for the timely escalation of cybersecurity incidents and vulnerabilities by "line" cybersecurity personnel to more senior personnel and those responsible for making disclosures. In addition, companies should ensure that they maintain and follow appropriate policies for vulnerability and patch management, as well as cyber incident response. Finally, following the decision of the Delaware Supreme Court in *Marchand* v. *Barnhill*,[11] companies should consider whether the responsibility for oversight of cybersecurity risks may be considered "essential and mission critical" in certain contexts, which may subject directors to a *Caremark*[12] claim for a breach of the duty of loyalty, exposing them to personal liability.

* * *

ENDNOTES

1 U.S. Securities & Exchange Commission, Press Release, *SEC Charges Issuer With Cybersecurity Disclosure Controls Failures* (June 15, 2021), *available at* https://www.sec.gov/news/press-release/2021-102.

2 First American Financial Corporation, Release No. 92176 (June 14, 2021), *available at* https://www.sec.gov/litigation/admin/2021/34-92176.pdf [hereinafter Order].

3 Exchange Act Rule 13a-15(a), (e).

4 *Id.*

5 Order, *supra* n.2, at 6.

6 New York Department of Financial Services, Press Release, *Department of Financial Services Announces Cybersecurity Charges Against a Leading Title Insurance Provider for Exposing Millions of Documents With Consumers' Personal Information* (July 22, 2020), *available at* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221. For additional information on the DFS action, see our Client Memorandum "New York State Department of Financial Services Announces First Enforcement Action Under Cybersecurity Regulations," dated July 31, 2020, *available at* https://www.sullcrom.com/files/upload/SC-Publication-New-York-DFS-Announces-First-Cyber-Enforcement.pdf. The DFS has since amended and expanded the charges against First American. *See* Amended Statement of Charges and Notice of Hearing, No. 2020-0030-C (Mar. 10, 2021), *available at* https://www.dfs.ny.gov/system/files/documents/2021/03/ea20200721_first_american_notice.pdf.

7 New York Department of Financial Services, Public Hearings and Decisions, *available at* https://www.dfs.ny.gov/reports_and_publications/public_hearings (last visited June 17, 2021).

8 U.S. Securities & Exchange Commission, Cybersecurity Enforcement Actions, *available at* https://www.sec.gov/spotlight/cybersecurity-enforcement-actions (last visited June 17, 2021); U.S. Securities & Exchange Commission, Commission Statement & Guidance on Public Company Cybersecurity Disclosures, Release No. 10459 (Feb. 21, 2018), *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

9 Exec. Order No. 14,208, 86 Fed. Reg. 26633 (May 12, 2021), *available at* https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

10 The White House, Memorandum, *What We Urge You to Do to Protect Against the Threat of Ransomware* (June 2, 2021), *available at* https://www.whitehouse.gov/wp-content/uploads/2021/06/Memo-What-We-Urge-You-To-Do-To-Protect-Against-The-Threat-of-Ransomware.pdf.

11 212 A.3d 805 (2019) (refusing to dismiss a derivative action against an ice cream company's directors for failing to implement a system of monitoring or reporting related to food safety).

12 698 A.2d 959 (Del. Ch. 1996).

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.