King & Spalding

Client Alert

Providing Strategic Legal Guidance to the Global Financial Services Industry

FINANCIAL SERVICES

JULY 14, 2021

For more information, contact:

William Johnson
+1 212 556 2125
wjohnson@kslaw.com

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Matthew Hanson
+1 202 626 2904
mhanson@kslaw.com

Charles Cain
+1 202 626 5510
ccain@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

New York
1185 Avenue of the Americas
New York, New York 10036-4003
Tel: +1 212 556 2100

SEC Returns Spotlight to Cybersecurity Disclosure Enforcement

On June 15, the Securities and Exchange Commission announced a settlement with First American Financial Corporation for what the SEC found were inadequate disclosure controls and procedural violations, revealed in connection with a cyber incident last spring. Since the SEC published guidance in early 2018 regarding disclosure principles related to cybersecurity vulnerabilities, it appears to have taken care to be thoughtful in not second-guessing companies' good faith decisions about whether and when to disclose such vulnerabilities, bringing charges only in two cases where disclosure lagged awareness of the vulnerability by approximately two years. In the *First American* matter, however, the gap between awareness and disclosure was less than 6 months, but the SEC still found that the company's policies and procedures were inadequate.

The SEC's order in *First American* is consistent with its published guidance and public statements by SEC officials, all of which emphasized the need for company employees with knowledge of security vulnerabilities to share that information with those responsible for making SEC disclosures.

In a related development, recently the SEC's Enforcement Division sent information requests to what appears to be a wide range of companies asking about how they responded to a high-profile software vulnerability that came to light in late 2020 involving an information technology company. The information requests in this new Enforcement sweep also ask recipients to provide information about other compromises, including those that were not disclosed at the time.

With new Chair Gary Gensler now several months into establishing priorities at the SEC, it is possible that the *First American* settlement, in combination with the new Enforcement sweep, may

signal the SEC Enforcement Division's increasing scrutiny on cybersecurity disclosure policies and procedures.

SEC'S OVERSIGHT OF CYBERSECURITY

The SEC has two main independent bases for regulating cybersecurity issues.

First, the SEC seeks to ensure transparency and full disclosure in the securities marketplace. It has wielded its regulatory and enforcement power in a manner designed to require all securities issuers — i.e., public companies — to disclose material events relating to their cybersecurity programs and vulnerabilities. In short, securities issuers must disclose material cybersecurity lapses, breaches, and vulnerabilities just like they must disclose any other material corporate events. The SEC staff and the full Commission itself have issued guidance to issuers in recent years regarding how their disclosure procedures ensure that security officials with knowledge of vulnerabilities share such information with those responsible for making disclosures, as well as what those officials should consider when deciding whether or not to disclose a cyber event.

Second, the SEC's oversight of broker-dealers, investment advisers, and other regulated entities includes a number of requirements for those companies' controls around assets and data.[1] For example, Rule 30 of the SEC's Regulation S-P[2] — more commonly known as the "Safeguards Rule" — requires that those regulated financial services firms safeguard the personal data of their customers. The SEC's Division of Examinations checks for compliance with these rules as part of its regular examination program, and the Division of Enforcement has brought charges based on failure to comply with these rules.

FEBRUARY 2018 GUIDANCE ON CYBER DISCLOSURES AND CONTROLS

In February 2018, the Commission published guidance to securities issuers regarding disclosures of cybersecurity risks and disclosure controls.[3] That announcement effectively updated similar guidance provided in 2011 by the SEC's Division of Corporation Finance, which focuses on the SEC's issuer disclosure rules. [4] The guidance emphasized the fact that a number of general securities disclosure requirements can impose a duty upon securities issuers to disclose cybersecurity risks and incidents. The 2018 guidance listed three primary examples. First, registration statements "must disclose all material facts required to be stated therein or necessary to make the statements therein not misleading."[5] Second, periodic reports, such as annual Form 10-K filings and quarterly Form 10-Q filings, require disclosure of cybersecurity risks and incidents in particular sections. Third, current reports filed on Form 8-K are generally used to report important news occurring between the quarterly and annual periodic reports and can be used to "report the occurrence and consequences of cybersecurity incidents." The guidance did not, however, create a specific obligation to disclose all cybersecurity incidents in a current report filing.

The 2018 guidance also included a discussion of considerations for issuers weighing whether a particular cybersecurity issue is material. The guidance aimed to help issuers work through disclosure questions they might encounter. On the heels of several large-scale data breaches at public companies, the guidance reminded securities issuers that the SEC considers cybersecurity incidents to be important — and potentially material — events that could trigger a duty to disclose.[6]

The 2018 guidance also pointed out that companies should have in place controls and procedures to ensure that information about cybersecurity risks and incidents is escalated quickly enough, and to appropriate levels within the company, to allow for timely disclosure. The purpose of this disclosure system is to "enable senior management to make disclosure decisions and certifications and to facilitate policies and procedures designed to prohibit directors, officers, and other corporate insiders from trading on the basis of material nonpublic

information about cybersecurity risks and incidents."[7] The guidance further reiterated that executives must certify the design and effectiveness of their company's disclosure controls and procedures.[8]

CONNECTING CYBERSECURITY AND INTERNAL ACCOUNTING CONTROLS

Further sharpening its focus on cybersecurity-related controls, on October 16, 2018, the SEC issued an investigative report advising public companies that internal accounting controls should "reasonably safeguard company and, ultimately, investor assets from cyber-related frauds."[9] The report was based on the SEC Enforcement Division's investigations of nine companies that fell victim to cyber fraud due to "business email compromises" (BECs). In these incidents, fraudsters impersonated company executives or vendors, convincing company personnel to send large sums of money to bank accounts controlled by the perpetrators, costing those companies millions of dollars.

The October 2018 report underscored the need for both public companies and regulated entities to consider cybersecurity risks when designing, maintaining, and implementing effective internal accounting controls. Such measures should include scrutiny of employee email use and security protocols, vendor diligence and identification, and related review of payment methods and policies.

FIRST AMERICAN DATA BREACH

Until recently, the SEC's disclosure controls cases seemed to be limited to cases involving failures to disclose known breaches by as long as two years from discovery, as well as a few enforcement actions against regulated entities for violations of the Safeguards Rule.

On June 15, the SEC announced it had settled charges against real estate settlement services company First American Financial Corporation for inadequate disclosure controls and procedural violations, following a cyber incident that was disclosed approximately six months after the company became aware of it.[10]

First American's title insurance business provided more than 90% of the company's revenues and included the handling of real property data containing purchasers' and sellers' non-public personal information ("NPPI"), including financial information. First American used its proprietary EaglePro information system to send secure and non-secure information "packages." Secure packages were password protected while non-secure packages could be easily shared with third parties. A vulnerability in the EaglePro system that had apparently existed since 2014 allowed access to images of secure information, including NPPI, by simply changing the numbers sequentially in a non-secure EaglePro URL. In some cases, these images were cached by publicly available search engines.[11]

The SEC's administrative order found that First American information security personnel first became aware of this vulnerability in January 2019 when conducting a security test. The SEC found that, per the company's internal controls, the vulnerability should have been remediated within 45 days. Due to a clerical error, however, it was assigned a remediation period of 90 days, concluding on May 9, 2019.[12]

On the morning of May 24, 2019, cybersecurity journalist Brian Krebs contacted First American and informed it of the vulnerability.[13] Later that day, Krebs published an article on his blog about the vulnerability, which contained a quote from First American stating that it had learned of the vulnerability and shut down external access to EaglePro.[14] First American filed a Form 8-K with the SEC on May 28, 2019 to describe the vulnerability, but did not disclose that its personnel had been aware of the defect since January 2019.

According to the SEC's order, First American's Chief Information Security Officer and Chief Information Officer did not become aware of the vulnerability until May 24 and May 25, 2019, respectively. The company's CEO and CFO were not made aware that the vulnerability had been identified and was not remediated at the time they filed the 8-K on May 28, 2019.[15] As a result, the SEC charged First American with violations of Securities Exchange Act Rule 13a-15(a), which requires "every issuer of a security registered pursuant to Section 12 of the Exchange Act to maintain disclosure controls and procedures designed to ensure that information required to be disclosed by an issuer in reports it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms." Without admitting or denying the SEC's findings, First American agreed to cease and desist from future violations, and to pay a $487,616 fine.[16] The *First American* action signals that the SEC is not content to bring enforcement actions only in extreme cases where there is a lag of several years between awareness and disclosure of a security vulnerability, but will also do so when facts involve much shorter periods, in an effort to ensure companies install and follow adequate disclosure policies and procedures.[17]

NEW ENFORCEMENT SWEEP

In mid-June 2021, Enforcement staff sent information requests to a number of securities issuers and regulated entities, asking for information about the recipients' previously undisclosed compromises, especially related to a high-profile software vulnerability discovered in late 2020. Offering amnesty for reporting failures to disclose (subject to certain conditions), the information requests echoed similar prior sweeps conducted by the SEC's Enforcement Division. In 2016, the SEC announced charges against 72 firms following a sweep related to disclosure failures by municipal securities underwriters.[18] In 2019, the SEC charged 79 investment advisers as part of a sweep focused on undisclosed conflicts of interest in the sale of certain mutual fund shares.[19] Although the new cyber-related sweep appears to be in a preliminary stage, the close timing between the sweep and the *First American* action suggests that the Enforcement Division may be intensifying its focus on cybersecurity disclosures and disclosure controls.

CONCLUSION

New SEC Chair Gary Gensler pledged in one of his first public speeches after being confirmed that the Commission would continue to stay abreast of evolving technology and would be ready to bring cyber-related enforcement cases.[20] In coming years, we expect the SEC will continue focusing on cybersecurity issues by issuing additional guidance, engaging with regulated firms during examinations, and commenting on issuers' cybersecurity disclosures. If the *First American* case and the new Enforcement sweep are a harbinger of things to come, however, the SEC's cybersecurity agenda may also now include increasing enforcement efforts in this area.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	FRANKFURT	LOS ANGELES	RIYADH	TOKYO
ATLANTA	CHICAGO	GENEVA	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
AUSTIN	DENVER	HOUSTON	NORTHERN VIRGINIA	SILICON VALLEY	
BRUSSELS	DUBAI	LONDON	PARIS	SINGAPORE	

[1] The Identify Theft Red Flags Rule (Regulation S-ID) also requires certain SEC-regulated entities to have a program to detect, prevent, and mitigate identity theft. 17 C.F.R. § 248.201. And Regulation Systems Compliance and Integrity (Regulation SCI) requires certain market-critical entities to have policies and procedures that ensure their systems have adequate capacity, integrity, resiliency, availability, and security. 17 C.F.R. § 242.1000-1007; *Staff Guidance on Current SCI Industry Standards*, U.S. SEC. & EXCHANGE COMMISSION (November 19, 2014), https://www.sec.gov/rules/final/2014/staff-guidance-current-sci-industry-standards.pdf.

[2] 17 C.F.R. § 248.30.

[3] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, U.S. Sec. & Exchange Commission (February 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[4] *CF Disclosure Guidance: Topic No. 2*, U.S. SEC. & EXCHANGE COMMISSION (October 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[5] The 2018 guidance stated, "The Commission considers omitted information to be material if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available."

[6] Some issuers have also chosen to engage in comment letter exchanges with the SEC, where the SEC staff has provided individualized guidance to issuers about potential disclosures.

[7] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, U.S. Sec. & Exchange Commission, supra note 3 at 18-9.

[8] 17 CFR 240.13a-14; 17 CFR 240.15d-14; 7 17 CFR 229.307; 17 CFR 249.220f.

[9] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements*, Exchange Act Release No. 844429 (October 16, 2018), https://www.sec.gov/litigation/investreport/34-84429.pdf.

[10] Press Release, U.S. Sec. & Exchange Commission, SEC Charges Issuer With Cybersecurity Disclosure Controls Failures (June 15, 2021), https://www.sec.gov/news/press-release/2021-102.

[11] *In the Matter of First American Financial Corporation*, Exchange Act Release No. 92176 (June 14, 2021), https://www.sec.gov/litigation/admin/2021/34-92176.pdf.

[12] *Id.* at 3-4.

[13] *Id.* at 4.

[14] Brian Krebs, *First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records*, KREBSONSECURITY (May 24, 2019), https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records.

[15] *First American Financial Corporation*, *supra* note 12 at 5-6.

[16] *Id.* at 6.

[17] The SEC's order follows charges announced by the New York Department of Financial Services ("NYDFS"), which launched its first ever cybersecurity enforcement action against First American for the EaglePro vulnerability in July 2020. First American has vowed to defend itself against the NYDFS charges in the upcoming administrative hearing. *See* William F. Johnson et. al, *Spotlight on DFS Trial Forum for First Cyber-Regs Case*, NEW YORK LAW JOURNAL (Mar. 3, 2021, 12:45 PM), https://www.law.com/newyorklawjournal/2021/03/03/spotlight-on-dfs-trial-forum-for-first-cyber-regs-case/.

[18] Press Release, U.S. Sec. & Exchange Commission, SEC Completes Muni-Underwriter Enforcement Sweep (Feb. 2, 2016), https://www.sec.gov/news/pressrelease/2016-18.html.

[19] Press Release, U.S. Sec. & Exchange Commission, SEC Share Class Initiative Returning More Than $125 Million to Investors (March 11, 2019), https://www.sec.gov/news/press-release/2019-28.

[20] *Remarks at 2021 FINRA Annual Conference*, SEC Chairman Gary Gensler (May 20, 2021), https://www.sec.gov/news/speech/gensler-finra-conference.