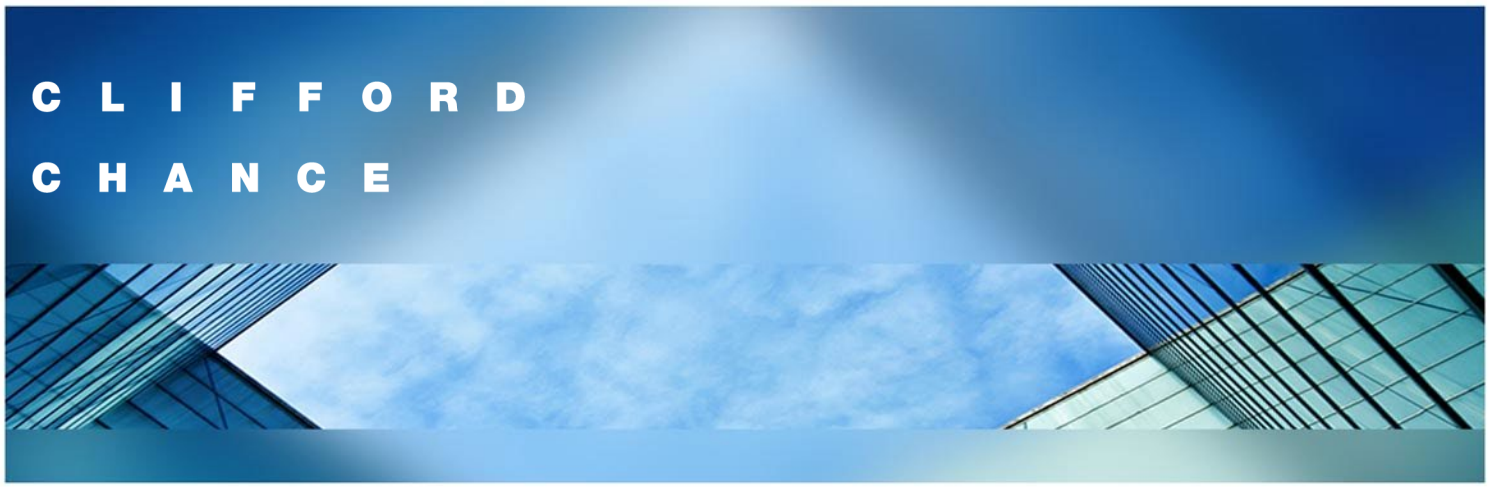

SEC ENFORCEMENT ACTION AGAINST FIRST AMERICAN UNDERSCORES IMPORTANCE OF ACCURATE DISCLOSURES OF CYBERSECURITY RISK

Signalling the increasing risks companies face not just from cybersecurity breaches but also disclosures about those vulnerabilities, the Securities and Exchange Commission ("SEC") announced a settlement with First American Financial Corporation on June 15, 2021, regarding a cybersecurity vulnerability in the company's systems that exposed hundreds of millions of financial documents, many of which contained sensitive personal data such as social security numbers and financial information. First American agreed to an approximately USD 500,000 civil penalty along with an order to cease and desist from committing or causing future violations. Of note, the SEC charges against First American were not based on inadequate cybersecurity; rather, the Commission fined the issuer for inaccurate and incomplete public disclosures stemming from the company's failure to ensure that senior executives were adequately informed of the vulnerability and the resulting risk to the company. The settlement underscores how important it is for senior executives to stay informed about a company's cybersecurity health.

Key issues

- The SEC fined an issuer USD 500,000 for improper disclosures relating to a cybersecurity vulnerability that exposed sensitive personal information of customers.
- Senior executives disclosed the vulnerability as soon as they were informed, as required by SEC rules. However, they later learned that company IT personnel had learned of the vulnerability months earlier.
- The settlement underscores the importance of ensuring senior executives stay informed about a company's cybersecurity health, and of making sure public disclosures about vulnerabilities are accurate and complete.

SEC RECORDKEEPING REQUIREMENTS

Rule 13a-15 of the Exchange Act requires any issuer of a security registered under to Act to "maintain disclosure controls and procedures" designed to ensure that required disclosures are timely reported pursuant to the Commission's rules. Among these rules are those relating to Form 8-K, which companies use to make required public reports regarding certain significant events that can have a material impact on the company, such as key personnel changes, major new contracts, and material impairments in the companies assets—including, in this

case, a cybersecurity vulnerability that may give rise to significant liabilities. Form 8-K reports must be filed within four business days after occurrence of the event.

THE ENFORCEMENT ACTION

According to the SEC order, the civil penalty arose from events relating to a cybersecurity vulnerability in First American's EaglePro application. EaglePro is a proprietary application First American uses to share images of title and escrow documents with its customers. This system contains 800 million document images for customers dating back to at least 2003, many of which display sensitive personal information such as social security numbers, bank account numbers, tax records, and other financial information.

On May 24, 2019, a prominent cybersecurity journalist notified the company that its EaglePro application had a vulnerability that allowed unauthorized users to view documents to which they should not have had access. First American provided the journalist with a statement explaining that they had taken immediate action to address the vulnerability and shared the statement with national media outlets that evening. A few days later on May 28, First American issued a Form 8-K describing the vulnerability, along with a press release.

After First American issued its May 28 Form 8-K, senior executives responsible for the disclosures learned that in fact information security personnel at the company had identified the vulnerability as early as December 2018, following a penetration test and security assessment of the EaglePro application. After identifying the vulnerability, IT personnel issued a report in January 2019 describing the vulnerability and recommending remedial action. However, despite company procedures requiring such vulnerabilities to be addressed within 45 days, the security weakness remained unaddressed. First American's Chief Information Officer and Chief Information Security Officer learned of the January 2019 report and the lack of subsequent remediation for the first time in the days following the May 24 report.

Unfortunately, neither officer informed senior executives in charge of issuing the Form 8-K that the vulnerability had been discovered months earlier, despite participating in numerous meetings with senior executives (including the CEO and CFO) in the days before May 28. As a result, the senior executives responsible for the Form 8-K disclosures were not able consider whether to disclose that the EaglePro vulnerability had been discovered months earlier. More broadly, the SEC order concluded that the responsible executives had not had sufficient information to fully evaluate the magnitude of risk the company faced as a result of the vulnerability when they approved the company's disclosures.

CONCERN ABOUT PILING ON?

The SEC enforcement action is the first penalty First American has faced related to the incident, but it is not the first complaint. In July 2020, the New York Department of Financial Services (NYDFS) issued charges against the company for multiple violations of the Department's Cybersecurity Regulation, 23 NYCRR 500.[1] The complaint is scheduled for a hearing in August 2021, after several

[1] For more on the NYDFS complaint, see our prior briefing here. The NYDFS complaint charges First American Title Insurance Company, the subsidiary of First American Financial Corporation that was affected by the cybersecurity vulnerability.

postponements potentially related to an expanded complaint issued by the Department in March 2021 that includes additional details regarding alleged violations of the Cybersecurity Regulation. Meanwhile shareholders and consumers have filed proposed class actions against the company relating to the cyber incident and the collateral effect the breach had on the company's share price. These different complaints—joined now by the SEC settlement—show the increasing risk companies face from cybersecurity vulnerabilities.

CONCLUSION

The SEC settlement is also an important reminder that cybersecurity issues cannot be left to IT specialists. The First American penalty was issued not because the company had inadequate cybersecurity controls; rather, the SEC took issue with the fact that senior executives were not informed of the vulnerability before making required public disclosures. Companies should ensure that senior executives—particularly those responsible for making required disclosures—are informed when cybersecurity issues arise that have the potential to give rise to significant liabilities.

Good cyber hygiene and risk management starts long before an incident occurs, and it is a global issue for multinational companies. Clifford Chance has published a number of reports and briefings to help companies protect themselves from attacks and vulnerabilities. For more information, see our Report on What Cyber Regulators Are Saying Around the World as well as our Ransomware Playbook. Also see our briefing here for more information on making required SEC disclosures.

CONTACTS

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Steven Gatti
Partner

T +1 202 912 5095
E steven.gatti
@cliffordchance.com

Benjamin Berringer
Associate

T +1 212 878 3372
E benjamin.berringer
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.