June 17, 2021

A New Angle on Cybersecurity Enforcement from the SEC

In recent years, companies across a wide range of industries have wrestled with the challenge of making appropriate disclosures about cybersecurity risks and vulnerabilities. Earlier this week, an SEC enforcement action, *In the Matter of First American Financial Corp.* (June 14, 2021) ("FAFC"), shed important new light on these cyber disclosure issues. Importantly, the case did not involve a third-party attack or actual data breach. Rather, it arose from an existing weakness in FAFC's systems, and centered on the company's public statements when the vulnerability was publicized in a press report. The case charges that FAFC failed to maintain disclosure controls and procedures sufficient to ensure that all available relevant information concerning the problem was analyzed for inclusion in the company's disclosures. The SEC has not previously employed this theory as the exclusive basis for a cyber-related enforcement action. FAFC settled without admitting or denying the SEC's findings.

FAFC is a real estate settlement services provider. According to the SEC's order, in mid-2019, a cybersecurity journalist contacted FAFC seeking comment on a story about a security vulnerability in one of the company's web-based applications. FAFC provided a statement to the reporter and also released it to other media outlets, noting, among other things, that "security, privacy and confidentiality are of the highest priority, and we are committed to protecting our customers' information. The company took immediate action to address the situation . . . ." Shortly thereafter, FAFC filed a Form 8-K, in which it stated that it "shut down external access to a production environment with a reported design defect that created the potential for unauthorized access to customer data."

According to the SEC, FAFC's information security personnel had identified this security vulnerability months before the journalist's inquiry. Despite detecting the problem, the company did not remediate it over the ensuing months. Moreover, in the immediate efforts to formulate a response to the May 24 inquiry, senior FAFC technical experts with knowledge of the earlier detection did not bring it to the attention of FAFC's senior executives responsible for disclosure, including the CEO and CFO. The SEC concluded that the senior executives consequently lacked information necessary to "fully evaluate the company's cybersecurity responsiveness and the magnitude of the risk" at the time they approved the disclosures.

Significantly, the SEC did not charge FAFC with antifraud violations, in contrast to the *Lumber Liquidators* case two years ago, which involved knowing or recklessly false statements in response to a corporate crisis, though not in the cybersecurity context. The SEC also did not charge FAFC under the theory spelled out in its October 2018 Report of Investigation concerning cyber-related frauds, which suggested that a failure to maintain adequate protections against cybercrime could constitute a violation of the internal controls provisions of the Exchange Act. Rather, the SEC charged FAFC with violating Rule 13a-15(a), for failure to maintain adequate disclosure controls and procedures. In addition to the specific failure in responding to the press inquiry, the SEC noted that FAFC did not have any disclosure controls and procedures related more generally to cybersecurity incidents. The SEC previously highlighted the importance of such controls, including the need to assure that information is communicated "up the corporate ladder" for disclosure purposes, in its *Statement and Guidance on Public Company Cybersecurity Disclosures* issued in 2018.

The SEC has recognized that it is not generally in the public interest to subject companies to enforcement action after they have been victimized by cyber incidents. *FAFC* illustrates that companies can compound their exposure, however, if they make public statements about cybersecurity risks and vulnerabilities, as well as efforts to address such factors, without sufficient examination of the relevant facts. This danger is magnified in a corporate crisis, when pressures to make reassuring statements may be most intense.

John F. Savarese
Wayne M. Carlin
Sabastian V. Niles