Davis Polk

SEC Cybersecurity Guidance and Commissioner Comments in the Context of an SEC Cybersecurity Enforcement Case Related to Insider Trading

March 16, 2018 | Client Update | 4-minute read

The SEC cybersecurity guidance, which we discuss in this client memo, reminds companies that their directors, officers and "other corporate insiders" should be aware that they may violate securities laws if they trade company securities while possessing knowledge of a company's cybersecurity risks and incidents before that becomes public information.

The guidance address some specific actions to review to mitigate the risks of insider trading. It encourages companies to consider (a) how their codes of conduct and insider trading policies take into account and prevent trading on the basis of material nonpublic information about cybersecurity matters; (b) whether and when it may be appropriate to implement restrictions on trading during investigations of cybersecurity incidents before breaches are made publicly known; and (c) adopting "prophylactic measures" through policies and procedures to protect against insider trading in these cases. Finally, the guidance notes that companies would be "well served" by evaluating how to "avoid the appearance" of improper trading from the period after discovering an incident and before making public disclosure.

In a recent speech, Commissioner Jackson questioned whether boards of directors are doing enough to ensure that companies have sufficient procedures such that whenever any member of senior management learns of material nonpublic information, all members of the team avoid trading. He referred to a study that he worked on prior to joining the Commission that identified a surprising amount of trading by corporate insiders during the four-day period between the time when material nonpublic information was discovered and when it was revealed to the public.

As for disclosure, he criticized the Commission's guidance for relying "heavily on the judgments of corporate counsel," given that "these judgments have, too often, erred on the side of nondisclosure, leaving investors in the dark—and putting companies at risk." He and his staff examined the 81 companies that reported breaches in 2017 to state and local regulators, as well as to the press, and found that only two of those companies filed 8-Ks disclosing the breach. He has asked that the SEC "give careful consideration to new 8-K requirements governing cyber events."

This attention on cyber breaches and insider trading may be in part due to the enforcement case against the chief information officer (the CIO) of a business unit at Equifax for improper insider trading. According to the complaint, the CIO was not informed of the cyber breach incident against the company. He was instead part of a separate project team that was told it was working on responses to a cyber breach that had occurred at an unnamed client, as part of a business opportunity. The teams were kept apart to limit the number of people who knew the company had been breached.

Through making some inquiries and from various internal communications, it appeared that the CIO was able to deduce that the company itself was the actual victim of the breach, as many of the requests and scope of work on his project appeared to be "highly unusual," according to the complaint. The CIO first became involved with his project team Friday afternoon. On Monday morning, he used a search engine to find information about the impact that a breach at another major credit bureau had on that company's stock price in 2015. The search of that other company's market data revealed that the company's stock price dropped about 4% after the public announcement of the breach.

Within an hour of running the Internet searches, the CIO exercised all of his vested options to buy, and then immediately sell, company shares, for total proceeds of a little less than a million dollars. Two days later, the CIO was told of the breach and instructed by an attorney that the information was confidential and that he should not trade in company securities. The attorney was unaware that the CIO had already traded. The company did not know of the CIO's trades until about a month and a half after publicly disclosing the incident. By selling in advance of public news, the CIO avoided more than $117,000 in losses.

The SEC determined that the CIO owed a duty of trust and confidence to his employer and shareholders not to trade on the basis of material nonpublic information that he learned through his employment, and knew or was reckless in not knowing that the information that the company had been the victim of a major cybersecurity breach was material and nonpublic.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Ning Chiu
+1 212 450 4908
ning.chiu@davispolk.com
