THE WALL STREET JOURNAL.

May 15, 2018

RISK & COMPLIANCE JOURNAL.

Cybersecurity Whistleblowers Are Growing Corporate Challenge

By Henry Cutter

SEC guidance gives tipsters reason to believe that by flagging a cybersecurity issue, they would also be highlighting a securities violation.

Signals from the U.S. Securities and Exchange Commission over how seriously it takes cybersecurity, combined with a Supreme Court ruling on whistleblower protections, are putting pressure on companies to be more careful about how they deal with potential tipsters, lawyers say.

The securities regulator issued guidance in February on how companies should handle cybersecurity issues. In April it fined Altaba Inc., formerly Yahoo Inc., $35 million over its handling of a 2014 hack, marking the first time the SEC penalized the victim of a breach.

"It's going to incentivize people inside an organization to step forward and disclose," said Brian Mahany, a whistleblower lawyer and founder of Mahany Law LLC. "I think the SEC is saying to

"It's going to incentivize people inside an organization to step forward and disclose," said Brian Mahany, a whistleblower lawyer and founder of Mahany Law LLC. "I think the SEC is saying to companies, 'We're taking this seriously. You take it seriously.

Continued on next page

Continued from previous page

companies, 'We're taking this seriously. You take it seriously.'"

Two of the five SEC commissioners—Kara Stein and Robert Jackson Jr.—said after the guidance was released that the agency hasn't gone far enough, a sign of pressure from the top to deal with cybersecurity concerns.

Cybersecurity isn't new ground for the SEC. The agency issued guidance in 2011 saying while no rules explicitly address cybersecurity-related disclosures, more general requirements may oblige firms to release information. Many companies responded by telling investors more about the danger they faced from hackers, but the risk has continued to grow. That prompted the SEC to weigh in again, the agency said.

"I definitely think this is a growth issue," for companies, said Dallas Hammer, an attorney at Zuckerman Law who represents employees in whistleblower matters. "We're getting [inquiries] about this every week."

The February guidance is "definitely much more pointed," said Mr. Hammer. It says companies' internal controls should enable them to prevent and detect breaches, assess their significance and make sure they are properly disclosed. Keeping insiders from trading on nonpublic knowledge about breaches is also a focus of the guidance, he said.

That gives whistleblowers reason to believe that by telling authorities about a cybersecurity problem, or a company's failure to disclose one, they would be reporting a securities-law violation. People who blow the whistle are protected from retaliation under the 2002 Sarbanes-Oxley Act and the 2010 Dodd-Frank Act if they believe they are reporting violations of SEC rules.

"This is significant if you have a blocking point in your chain of reporting," for cybersecurity issues, said Alexis Ronickher, a plaintiffs' lawyer at the whistleblower law firm Katz Marshall & Banks LLP.

A Supreme Court decision in February adds to the challenge for companies, said Gregory Keating, who heads the whistleblower-defense practice at the Boston law firm Choate Hall & Stewart LLP. The court decided antiretaliation provisions under Dodd-Frank apply only to individuals who flag potential wrongdoing to the SEC.

Just reporting problems in-house at work isn't enough, so whistleblowers are now more likely to go to the agency, said Mr. Keating. And employers may not know a staff member has gone to the SEC until the regulator approaches them about allegations.

To ease the path for workers to raise concerns internally, companies should open multiple channels for reporting, Mr. Keating said. Another step would be to train managers to know part of their job is to to recognize and deal with whistleblowers' concerns, and to evaluate them on how good they are at handling complaints,

One challenge is information-technology staff are responsible for both discovering cybersecurity issues and dealing with them, he said. A manager who receives a complaint about security from the IT staff may not realize that amounts to an instance of whistleblowing. But after that point any negative action—a bad performance review, for example—against the worker could give rise to a claim of retaliation.

"Employers need to be vigilant," Mr. Keating said.

Perhaps the most important steps, Mr. Hammer said, are making sure a whistleblower isn't treated differently after coming forward with a potential problem, raising concern about retaliation, and creating confidence among staff that management will seriously address concerns.

"That's going to keep most people from coming to me," he said. "Most people don't want to be whistleblowers." ■