**Portfolio Media. Inc.** | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# Investors Could Find Litigation Success With Equifax Breach

By **Carmen Germaine**

Law360, New York (September 11, 2017, 8:53 PM EDT) -- While investors have a pretty dismal track record at bringing shareholder class actions and derivative suits in the wake of data breaches, a confluence of factors at Equifax, including a sharp stock price drop and suspiciously timed trading, could make the credit monitoring company's massive hack fodder for securities liability.

Since revealing on Thursday that hackers accessed personal data on 143 million U.S. consumers, Equifax has already been hit with numerous class actions alleging the company failed to protect consumers' sensitive information, and experts said a wave of securities litigation is sure to follow.

Few public companies previously hit by cyberattacks have experienced significant stock drops, and accordingly, only a handful of shareholder class actions have been filed in the wake of data breaches. But Equifax's stock price opened nearly 15 percent lower the day after the attack was revealed, a drop that Hofstra University Maurice A. Deane School of Law professor Ronald J. Colombo ascribed to the magnitude of the breach.

"The enormity of the size of the breach, and the fact that it happened to one of the big three credit reporting agencies, an agency entrusted to have this type of information and keep it safe, I think that's what makes it shocking, so I'm not surprised the market reacted strongly," Colombo said.

Shareholder derivative suits alleging the board of directors of hacked companies failed to prevent attacks are more common, though they've met with little success in the past.

But experts said Equifax could present a unique case on that front as well if shareholders are able to point to share sales made by senior company executives just days after the breach was discovered to back up derivative claims. Meanwhile, the insider sales, as well as some unusual options trading, could attract the attention of the U.S. Securities and Exchange Commission.

While investor class actions related to data breaches are still rare, public companies including Target, Home Depot, Wendy's and Yahoo have been hit with derivative suits alleging their boards of directors made poor security decisions or failed to prevent attacks.

But those types of claims have a poor track record — while a suit against Yahoo continues, the derivative claims against Target and Wendy's were dismissed. Home Depot settled its derivative claims by implementing a series of policy reforms and agreeing to pay $1.125 in attorneys' fees but only after the suit had been dismissed and was on appeal.

Douglas W. Greene, chair of the securities litigation practice group at Lane Powell PC, said that shareholder derivative claims alleging company directors breached their duties are particularly difficult to bring.

"The shareholder has to plead intentional wrongdoing to plead a substantial likelihood of liability in the case of a director oversight claim," Greene said. "That's a high hurdle."

Colombo noted that shareholders alleging derivative claims have little chance of success unless

Colombo noted that shareholders alleging derivative claims have little chance of success unless they can show a conflict of interest or fraud on the part of the directors themselves, which is unlikely in Equifax's case, where the company's data was breached by an outside hacker.

But Equifax shareholders do have one unusual avenue to take in a derivative suit that could make this case different. After the breach was announced, media reports revealed that three Equifax officers sold chunks of their shares in the company in early August, days after the company became aware of the attack.

According to filings Equifax made with the SEC, Chief Financial Officer John Gamble, President of U.S. Information Solutions Joseph Loughran and President of Workforce Solutions Rodolfo Ploder collectively sold about $1.8 million in Equifax shares on Aug. 1 and 2, several business days after the company discovered the breach on July 29.

Those trades, which were not reported as part of scheduled trading plans, could leave Equifax vulnerable to an SEC investigation into whether the executives illegally traded on inside information, as well as a derivative suit seeking to force the executives to cough up any profits they made on the sales.

An alert from whistleblower firm Constantine Cannon LLP noted that the trades could be an example of insider trading and that knowledge about any insider trading "may be of interest to the SEC whistleblower program."

But experts said it's unlikely that the executives, who are required to publicly disclose such trades, would have engaged in trades after learning of the breach. Equifax did not immediately return a request for comment, but an Equifax spokeswoman told Bloomberg that the executives had no knowledge that the breach had occurred when they made the trades.

Steve Crimmins, a partner at Murphy & McGonigle PC, said Equifax likely would only make such an affirmative statement denying any insider trading if it had investigated the trades and were certain the executives were unaware of the breach at the time.

"It's unusual for a company to do that," said Crimmins, a former SEC enforcement attorney. "To me, I think it's likely to mean that the company and its lawyers have gotten on top of the situation quickly."

The SEC will likely perform its own investigation to verify that the CFO and the other executives didn't trade on inside information, Crimmins said, but if everything checks out, the agency is unlikely to bring a case as insider trading charges require an awareness of the material nonpublic information at issue.

On the other hand, experts said that if it's true the executives weren't aware of the breach, shareholders could claim in a derivative suit that Equifax lacked sufficient internal controls. Colombo noted that companies have a duty to put in place systems of controls and reporting, designed to prevent, detect and report up situations like a data breach.

"To the extent that they don't, and to the extent that the CFO's going to claim, 'I didn't know this happened' even though it happened four days earlier, that would appear to suggest that their systems aren't that robust," Colombo said.

John Reed Stark, the president of cybersecurity firm John Reed Stark Consulting LLC and former chief of the SEC's Office of Internet Enforcement, said that in general, companies should be engaging their C-suite on many levels as soon as possible after a breach is discovered. On the financial side, a breached company will immediately be spending large sums of money on a response and making important financial choices, as well as working with its insurer.

"Most data breaches that I'm involved in, there is active C-suite engagement because of bet-the-company issues and the dynamic nature of the issues," Stark said.

Of course, shareholder derivative suits remain difficult to bring, and it's possible any derivative claims against Equifax will have as little success as those brought against other hacked companies.

While derivative claims have largely been dismissed, few investors have even bothered bringing a securities fraud class action after a data breach as few public companies hit by cyberattacks have experienced significant stock drops.

"For the most part, cybersecurity breaches have not yielded securities class actions because, in general, stock prices haven't fallen a significant amount after the disclosure of a breach," said Greene. "That's bound to change."

At least two plaintiffs firms, The Rosen Law Firm PA and Block & Leviton LLP, have issued shareholder solicitations announcing they are investigating whether Equifax or its board violated securities laws in the run-up to the breach. Such litigation would likely focus on whether Equifax's previous disclosures related to its cybersecurity were false or misleading — for instance, whether the firm boasted about its cyber protections when it knew or should have known about significant vulnerabilities.

Noel Chandonnet Jr., the director of institutional investor marketing at The Rosen Law Firm, said that while it's premature to say whether his firm will file a suit, they're currently checking into whether Equifax's security was deficient and whether any deficiencies heightened the company's exposure to a cyberattack.

"Because if it did, then public statements they've made regarding their data security would have been false and misleading," Chandonnet said. "Again, we're just looking into it."

Chandonnet referred to an investor publication Equifax released on Aug. 16 — two weeks after the company became aware of the breach — in which it claimed to "serve as a trusted steward and advocate for our customers and consumers," and said it was making "continued investments to address critical data security throughout the company."

Investors could also focus on whether Equifax waited too long to disclose a breach. In the Yahoo investor action, for example, plaintiff shareholders have alleged in part that Yahoo committed securities fraud by "knowingly withholding information about the two largest data breaches in history."

Whether that claim will get traction in Equifax's case is unclear. Companies that have been victimized by a cyberattack need to disclose the breach quickly if it was material to their operations, experts said, but they also have to gather enough information to ensure any disclosure isn't false or misleading.

"A company will want to have a good understanding of what actually happened before releasing potentially inaccurate information to the market," said Joseph B. Crace Jr., co-chair of Bass Berry & Sims PLC's securities and shareholder litigation practice group. "So there's a bit of a delicate balance between acting too quickly or acting too slowly."

Investors also may not be the only parties looking at Equifax's securities liability. Beyond any investigation of the executive stock sales, the SEC may be interested in reports that trades made in Equifax options in August generated more than $4 million in profits once the breach was disclosed — and whether those trades were made on the basis of inside information.

The agency could also be looking at Equifax's statements related to its cybersecurity. Although the SEC has yet to bring an enforcement action over misleading or false cybersecurity disclosures, staff have certainly not ruled out such a case, and Enforcement Division Co-Director Stephanie Avakian said last week that she "could envision a matter where a case would be appropriate."

Crimmins said the SEC will "deliver on its promise to take action," given how seriously the agency's staff is taking cybersecurity. But he added that, although cybersecurity has become a central concern for all businesses, the SEC also recognizes that breaches are always possible despite the efforts of any business.

"When bad people are using incredibly sophisticated technology to break into your operation, it's like robbing a bank — you do your best, and the bank does its best to protect the vault, but sometimes despite best efforts, there can be a robbery," Crimmins said. "The question really is:

sometimes despite best efforts, there can be a robbery," Crimmins said. "The question really is: Have the institutions involved done their best to protect their data? And if they have, then not every breach is going to be the occasion for blame."

--Editing by Christine Chun and Aaron Pelc.

All Content © 2003-2017, Portfolio Media, Inc.