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

Equifax Ruling Shows How Cyber Boasts Can Bring Legal Pain

By **Ben Kochman**

Law360 (January 31, 2019, 9:47 PM EST) -- A Georgia federal judge's ruling that Equifax investors can sue the infamously hacked credit reporting giant for touting its cybersecurity even after its hired consultants spotted glaring flaws may spark other companies to be more careful about how they talk about their own digital defenses.

In Monday's decision against the company and its former CEO Richard Smith, U.S. District Judge Thomas W. Thrash Jr. made clear that the mere fact of Equifax's historic breach was not enough to keep the stock-drop securities suit alive. Instead, he found the investors had crucially made "a multitude of specific, detailed factual allegations" beyond the breach, including that Smith had expressed concerns about a hack into company databases in an August 2017 speech at the University of Georgia without revealing what he already knew: that those fears had been realized.

Thrash's ruling provides a bit of a road map for what liability companies and their top executives might face from the growing list of similar stock-drop suits filed in the wake of data breaches, industry attorneys tell Law360. Google parent Alphabet Inc., chipmakers Intel Corp. and Advanced Micro Devices Inc., market research company Nielsen, and hotel giant Marriott International are among those currently facing suits claiming they mislead the market by making "false or misleading" public statements before they reported data episodes.

It will be worth watching in the coming months whether Equifax's legal troubles prompt other companies to be more open with the public about the risks of a cyberattack, whether in U.S. Securities and Exchange filings or other public documents, in order to avoid liability. And for executives — who can be held personally liable in a stock-drop suit — the judge's allowing the case against Smith to go forward is cause for using caution when talking about cybersecurity.

"Companies are going to be more careful about saying how good their cybersecurity is going forward," said Avi Gesser, a partner on Davis Polk & Wardwell LLP's cybersecurity and data privacy team. "I think this makes it even more important that, depending on your cyber risks, you alert your investors to the possibility that even if you take measures designed to protect data, those might not be successful."

"That's reality of life in 2019," he added. "Companies will be more careful about saying positive things about their cybersecurity without caveats."

In Equifax's case, Judge Thrash devoted much of his 109-page ruling to **describing** how the specificity of the company's representations about its data security could potentially deceive the market. He wrote that the company's assurance that it "employed a rigorous enterprise risk management program is more misleading to investors than simply affirming the existence of an enterprise risk management program." The judge rejected Equifax's claims that its statements were "vague, meaningless, statements of corporate optimism," and concluded that the importance of data security to a business like Equifax made it more likely that investors would deem these representations to be important.

"Hopefully this continues to underscore for companies everywhere that courts are taking this seriously, and that courts are going to look in a very detailed way at the facts to show clear corporate responsibility and expectations for what are reasonable actions here," said April Doss, a

corporate responsibility and expectations for what are reasonable actions here," said April Doss, a partner on the cybersecurity and privacy team at Saul Ewing Arnstein & Lehr LLP.

Part of that responsibility is keeping up with industry best practices, which the investor suit led by Union Asset Management Holding AG alleged Equifax failed to do before its September 2017 admission that hackers had exploited a website application vulnerability in its systems to access names, Social Security numbers, addresses and other personal data belonging to what ended up being more than 148 million people.

A third-party audit from cybersecurity firm Mandiant conducted around March 2017 found that Equifax's digital defenses were "grossly inadequate," with unpatched software flaws and poor password policies, according to the suit.

"C-Suite executives really need to recognize that the ostrich approach to cybersecurity just wont work," Doss said. "They can't put their heads in the sand and say 'we don't know,' because the court may say that you should have known that your cyber practices were far below industry standards."

Judge Thrash did ax claims against the other executives named in the case — Equifax Chief Financial Officer John Gamble Jr., Workforce Solutions President Rodolfo Ploder and former Senior Vice President Jeffrey Dodge — finding that there was no evidence they had been given any warnings or specific information about the company's cybersecurity deficiencies.

That decision could cause company bosses to think twice before getting briefed in cybersecurity discussions or discussing the issue in public, said VLP Law Group LLP partner Melissa Krasnow.

"The question is: Will this change how companies handle cybersecurity going forward? Will the CEO become less involved? Will CEOs speak about cybersecurity publicly, or will there be a chill and they will not speak about it as much as they have previously?" Krasnow said.

Another theme to watch in future cases are disputes over what sort of information can be traded in discovery in the early stages of suits. The level of public outcry spawned by the Equifax case led to information about what the company allegedly knew and when trickling out through a congressional investigation and media reports. Smith's speech at the University of Georgia, for example, drew a flurry of headlines after it was posted on YouTube.

It's unclear whether plaintiffs will have access to such a level of insight in future cases, which will likely lead to fights over, for example, whether cybersecurity audits prepared by third-party consultants at the behest of company lawyers should be sealed from view by attorney-client privilege.

"We can expect that corporate defendants will try to assert privilege and have consultants hired through counsel, and you'll see plaintiffs arguing that they need to see the fruits of those reviews in order to assess what the company's level of knowledge was," Doss said. "Those kinds of battles about what is privileged and therefore shielded from discovery are really central to the legal strategy in these cases going forward."

--Additional reporting by Allison Grande. Editing by Emily Kokoll and Alanna Weissman.