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 Insider Trading Charges Show Need For Action Plan

By **Jody Godoy**

Law360 (March 15, 2018, 5:44 PM EDT) -- Insider trading charges for a former Equifax executive involved in responding to a data breach affecting some 148 million customers illustrates the need for companies to have solid plans for dealing with cyberattacks that include adequate bulwarks against illegal trading, experts say.

When Equifax was breached last summer, Jun Ying was the chief information officer in its U.S. information systems unit. Although Ying was not actually told about the hack, he used his knowledge of the behind-the-scenes scramble in its wake to conclude that Equifax itself had been targeted and to trade on that information, according to criminal and civil cases announced on Wednesday.

David Axelrod, a former supervisor at the U.S. Securities and Exchange Commission and federal prosecutor who now practices at Ballard Spahr LLP, says it's the first time he's seen insider trading charges against an insider based on knowledge of a data breach.

Axelrod says the charges against Ying suggest that heightened precautions often used to prevent improper trading during corporate sales and acquisitions may also be appropriate for the information technology side.

"While most companies have broad insider trading policies, you'll see a new emphasis on warning people in data security divisions that insider trading policies apply to them," Axelrod said.

The case illustrates a point the SEC made three weeks ago when it launched cybersecurity guidance for publicly traded companies. The SEC urged companies to consider the risk of insiders capitalizing on their knowledge of a breach during the initial phase when a company has yet to alert the public.

Prosecutors and the SEC both claim Ying started working on a response to the breach on a Friday in August and "put 2 and 2 together" to sell off his Equifax stock before lunchtime the following Monday and avoid his shares losing more than $100,000 in value.

But the civil complaint also goes into a level of detail that allows for a post-mortem on Equifax's internal response and what it did to prevent employees from illegally cashing in.

In the weeks after Equifax first detected unusual site activity, the company formed a crisis response team with the nondescript moniker Project Sierra.

That team was privy to a finding that Equifax customers' data had been compromised and was told to keep the information under wraps. The SEC complaint hints that Equifax succeeded in putting the fear of the law into employees who did have actual knowledge of the breach.

The complaint asserts that Ying did not learn of the efforts from one of his peers who was tapped to lead remediation efforts. When Ying called the company's global CIO to ask why his team was suddenly slammed with work, the global CIO replied that Ying did not need to know, the SEC wrote.

The Project Sierra team was also subject to a blackout period banning them from trading on what they knew, according to the complaint.

But Ying was part of a secondary tech team dubbed Project Sparta that was working on a remediation plan including tools for customers to check whether they had been exposed. They were told they were working on a breach at an unnamed Equifax client, the SEC said.

Cam C. Hoang, a partner at Dorsey & Whitney LLP who formerly practiced in-house at General Mills Inc., said companies looking at this case should consider who is covered by blackout periods for crisis events and plan to clearly communicate expectations and points of contact like the company's general counsel.

After an event has occurred, it becomes more difficult to justify keeping knowledge from high-level executives involved in response, Hoang said. For Equifax, that would include information security executives who were key to remediating the breach, she said.

"The Equifax breach is a situation where we see the risk of not expanding the blackout broadly enough," Hoang said.

Top Equifax executives faced questions last year about their stock sales that fell within the period between when the company knew it had been hacked and when it told the public.

The company ultimately cleared those executives when a WilmerHale investigation showed they had not known about the breach and that their trades were vetted by the company's general counsel, as Equifax policy required.

According to the report on the top executives' trades, Equifax only required its GC to sign off on trades by directors and "certain senior Equifax officers."

The SEC emphasized Ying's seniority when it announced the case, noting he had been tapped to take over as the company's global CIO.

Crowell & Moring LLP partner Paul Rosen, who responded to government hacks in his former job at the U.S. Department of Homeland Security, noted that, in addition to broad insider trading policies, companies need processes to vet the trades of employees likely to have material information — a category often including senior executives.

Companies need to figure out where to draw the line, Rosen said.

Equifax had a blanket policy in place prohibiting employees trading on nonpublic information, and Ying had gotten an email around a month before the breach reminding him of that fact, according to the

criminal indictment. Prosecutors offered no detail, however, on the email or efforts to promote compliance with the program.

Rosen noted that anti-insider trading policies need to be accompanied by the right training to make them stick.

“Policies alone are not necessarily sufficient, they need to be trained on and practiced,” Rosen said. “You can’t just give someone a 400-page training manual every year and say, ‘review it.’”

Based on the allegations, attorneys saw the case as a tough one to defend.

One of the claims that former prosecutors called hardest to overcome is Ying’s online search on how the market responded to a data breach at Experian in September 2015. He saw that the company’s stock had dropped around 4 percent right before he traded in his own Equifax stock, according to the SEC.

“It’s a really deadly piece of evidence,” said Axelrod. “That piece alone suggests he knew there was a data breach and was contemplating trading but before he did it he wanted to know exactly how important the information was.”

Another hard pill to swallow for Ying’s defense is that he not only sold shares, he first exercised all of his thousands of vested stock options and then sold all of the stock without missing a beat, according to the government.

“That is a significant fact. I think it goes to his state of mind at the time of the trade and to ultimate issues around culpability,” said Rosen.

Hoang pointed out that an alleged text trail, in which Ying told his supervisor “I don’t want to know ;)” and another colleague “I think some big media announcement is coming about us,” doesn’t help his case, either.

But while Ying’s alleged trade to avoid a stock drop is legally the same as cashing in an illicit tip, different psychological forces are at work, said Justin C. Danilewitz, a former prosecutor and now partner at Saul Ewing Arnstein & Lehr LLP.

“It is very difficult for anyone to sit by idly and just observe a loss of great magnitude when they can avoid it,” Danilewitz said.

Companies looking to deter improper trading need to have employees take a moment to picture themselves in a situation like Ying’s, he said.

“Imagine you are about to lose $100,000. You have to have the strength of character to walk away and do nothing about it,” Danilewitz said. “The alternative is catastrophic loss much greater than the financial loss you will experience from not making a trade.”

--Editing by Brian Baresch and Orlando Lorenzo.