The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 31130

March 15, 2018

SEC Charges Equifax CIO with Insider Trading for Selling Shares Prior to Public Disclosure of Breach

[31130]

March 15, 2018 TO: ICI Members
Investment Company Directors
ICI Global Members
Chief Information Security Officer Advisory Committee
Chief Risk Officer Committee
Technology Committee SUBJECTS: Compliance
Cybersecurity
Litigation & Enforcement RE: SEC Charges Equifax CIO with Insider Trading for Selling Shares Prior to Public Disclosure of Breach

Summary of the SEC's Allegations

As you may recall, in September 2017, Equifax, one of three major credit bureaus, announced a massive data breach that exposed the social security numbers and other personal information of approximately 148 U.S. customers. Yesterday, the SEC filed a civil action against the Chief Information Officer (CIO) of Equifax alleging that he committed fraud under the Securities Act of 1933 and the Securities Exchange Act of 1934 by engaging in insider trading.[1] The SEC's Complaint, alleges that, following Equifax's discovery of the breach, but prior to it becoming public, the CIO exercised all of his vested Equifax stock options and then sold the shares. According to the SEC, these transactions resulted in proceeds of approximately $1 million and avoided more than $117,000 in loses.

Background [2]

The SEC's Complaint begins with Equifax spotting suspicious traffic on its network on July 29, 2017. This suspicious activity involved the portion of the company's website where consumers dispute items on their credit reports. It then discusses in detail Equifax's response to this suspicious traffic. It notes that, between the discovery of the breach in July and Monday, August 28th, the CIO was involved in limited aspects of Equifax's response to the breach without being fully informed that the firm had experienced a breach. Notwithstanding the fact that he had not been informed of the breach, the CIO "concluded that Equifax itself was the victim of a major cybersecurity breach, despite statements made [as part of Equifax's internal response] asserting that [the response] was a business opportunity for an unnamed client." [3] Apparently, once the CIO suspected Equifax had

been the subject of a breach, he "used a search engine to find information on the internet concerning the September 2015 cybersecurity breach of Experian[4] . . . and the impact that breach had on Experian's stock price."[5] Through these searches, the CIO discovered that, although Experian's breach was much smaller than the Equifax breach, "the public announcement of Experian's breach negatively impacted that company's stock price" and caused the price to drop approximately four percent.[6]

"[W]ithin an hour of running the internet searches regarding [the Experian breach, the CIO] exercised all of his vested options to buy Equifax shares and then immediately sold those shares . . .."[7] According to the Complaint, these transactions: were made on the basis of material nonpublic information; breached the duty of trust and confidence that the CIO owed to Equifax and its shareholders; and involved deceptive and fraudulent conduct.

On August 30th, two days after the CIO's trades, he was officially informed of the breach, told that information about the breach was confidential and should not be shared with anyone, and told that he should not trade in Equifax securities. The Complaint notes that the CIO "did not volunteer the fact that he has exercised and sold all of his vested Equifax options two days before."[8]

The public was informed of the breach when Equifax issued a press release and filed a Form 8-K with the SEC after the close of the market on September 7, 2017. Following this public notice, the price of Equifax common stock dropped nearly 14% and trading volume increased more than thirty-fold from the previous day's trades. On September 15, 2017, following the resignation of the then-current global CIO, the CIO was offered the position of global CIO of Equifax. This offer was withdrawn when senior executives of Equifax learned of the CIO's trading. On October 16, 2017, following an internal Equifax investigation into the CIO's trading, Equifax concluded that the CIO had violated the company's insider trading policy and that his employment should be terminated. The CIO instead resigned.

The SEC's Charges and Relief Sought

Based on the above allegations, the SEC charged the CIO with two counts of insider trading – one count for exercising his options to buy his vested stock options and one count for selling his shares in Equifax. The Compliant seeks: (1) a finding that the CIO violated the antifraud provisions of the federal securities law; (2) a permanent injunction against the CIO; (3) an order of disgorgement; (4) a civil monetary penalty; (5) an order prohibiting the CIO from serving as an officer or director of a public company; and (6) such other relief as the Court may deem just and proper. The SEC is seeking a trial by jury on its Complaint. According to a press release announcing the Complaint, the SEC's investigation of the matter is continuing and the U.S. Attorney's Office for the Northern District of Georgia is pursuing "parallel criminal charges" against the CIO.[9]

The SEC's Recent Guidance Relating to Insider Trading in the Wake of Cyber Event

It is worth noting that, on February 21, 2018, the SEC issued a press release announcing its adoption of a *Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*.[10] As described in the SEC's press release,

The guidance provides the Commission's views about public companies' disclosure obligations under existing law with respect to matters involving cybersecurity risk and incidents. It also addresses the importance of cybersecurity policies and procedures and the application of disclosure controls and procedures, insider trading prohibitions, and

Regulation FD and selective disclosure prohibitions in the cybersecurity context. [Emphasis added.]

With respect to the issue of insider trading, the Guidance reminds "companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material nonpublic information about cybersecurity risks or incidents."[11]

Tamara K. Salmon
Associate General Counsel

endnotes

[1] *See SEC v. Jun Ying* (U.S. D.C. N.D. GA), filed March 14, 2017, which is available at: https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf (the "Complaint"). Jun Ying was an employee of Equifax, Inc. from January 2013 until October 2017, and was the CIO of Equifax's United States Information Systems business unit at the time of his departure.

[2] The discussions of the facts of this case are taken from the allegations in the SEC's Complaint.

[3] Complaint at p. 11.

[4] Like Equifax, Experian was one of three major credit bureaus.

[5] Complaint at p. 12.

[6] *Id.*

[7] Complaint at p. 13.

[8] Compliant at p. 15.

[9] *See "Former Equifax Executive Charged with Insider Trading,"* SEC Press Release No. 2018-40 (March 14, 2018), which is available at: https://www.sec.gov/news/press-release/2018-40.

[10] *See "SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures,"* SEC Press Release No. 2018-22 (February 21, 2018), which is available at: https://www.sec.gov/news/press-release/2018-22. The SEC's Guidance is available at: https://www.sec.gov/rules/interp/2018/33-10459.pdf. The Guidance makes clear that it only applies to public companies and does not apply to registered investment companies of investment advisers. *See* Guidance at fn. 13.

[11] Guidance at p. 7.