## INSIDER TRADING

# You Might Be an Inside Trader if . . .

*Material non-public information is not limited to definitive information about the corporation. Equifax's former chief information officer is now facing insider trading charges because he traded after receiving information related to an anonymous cybersecurity event.*

*By Kari M. Rollins and Sarah E. Aberg*

Earlier this year, the Securities and Exchange Commission (SEC) released cybersecurity guidance addressing, among other things, the risk of insider trading in the event of a data breach.[1] The SEC's guidance pointed out that insider trading risk comes not just from the risk that the intruder will trade on stolen, non-public information, but also the risk that corporate insiders will trade on their knowledge of the breach itself. In this manner, the SEC has dived into the ever-growing pool of potential regulatory enforcers who may be quick to act in the event of a data breach. The SEC demonstrated its new capabilities in the recent insider trading case against Jun Ying, the former Chief Information Officer of Equifax's United States Information Systems business unit.[2]

## The Equifax Breach

On July 29, 2017, Equifax discovered that it had suffered a major cybersecurity breach. Equifax immediately launched a complex structure of internal teams to respond to the breach. However, only one team was informed that Equifax was the victim of the breach. The other teams were told they were working on a "business" or "breach" opportunity for an unnamed client. Initially, Equifax instituted a trading blackout, but only for its employees who were told of the breach. Ying was not on the team that was informed of the breach, and was not informed of the blackout. On August 28, 2017, Ying exercised all of his vested options to buy Equifax shares and immediately sold those shares for approximately $950,000. After the close on September 7, 2017, Equifax publicly disclosed the data breach. The following day, Equifax's stock price dropped. Had Ying waited to sell his shares until after the breach was made public, he would have earned $117,000 less on the sale.

## The Government's Argument: Ying Traded on Inside Information

This past March, the SEC and the Department of Justice (DOJ) brought securities fraud and insider trading charges against Ying in parallel civil and criminal actions. The complaints allege the following facts:

- Four days prior to the breach, on July 25, 2017, Ying received a reminder email that Equifax employees could not trade in Equifax securities if they were aware of material nonpublic information.
- Ying was aware that, between August 12 and August 15, 2017, Equifax changed internal administrative credentials for many internal databases.
- On August 25, 2017, Ying and several of his reports were asked to assist in responding to the breach. However, Ying and his reports were not informed that it was Equifax that had been breached. Instead, Equifax portrayed the work "as part of a breach opportunity involving a potential Equifax customer."

**Kari M. Rollins** *is a partner, and* **Sarah E. Aberg** *is an associate, at Sheppard, Mullin, Richter & Hampton in New York, NY.*

- That same day, Ying texted an Equifax colleague, "Sounds bad. We may be the one breached" and "I'm starting to put 2 and 2 together."
- The SEC complaint adds that Ying then spoke to Equifax's Global CIO, who told Ying he did not need to know why he was expected to assist with the "breach opportunity," but at some point, Ying would understand what was happening. Afterwards, Ying texted another colleague who had asked for his assistance on the "breach opportunity" that he had "[n]o question right now. Actually, I don't want to know;) I told the team to [rally]."
- The SEC complaint also adds that "[n]umerous additional communications the evening of August 25, 2017, informed Ying that this breach was unusual, and indicate that Ying used the information entrusted to him as an Equifax employee to conclude that Equifax was the victim of the breach, and that the 'breach opportunity' idea suggesting a client was the victim was merely a cover story." As support for this assertion, the SEC complaint goes on to reference (1) the unusually burdensome breach response plan for the "customer," (2) text messages in which Ying compares the breach response plan to Equifax's Crises Management Plan, (3) Ying's cancellation of travel plans the following week due to "all the mad scrambling....", and (4) his instruction to one of his reports to "cooperate" with a request from Equifax's Senior Director of Crisis Management asking for log files for a specific database.
- The following work day, August 28, 2017, Ying performed three internet searches: "experian breach"; "experian stock price 9/15/15"; and "experian breach 2015."
- Shortly after he performed the searches, Ying exercised his Equifax stock options to buy Equifax shares and immediately sold those shares for approximately $950,000, for a realized gain of $480,000.
- The next day, August 29, 2017, Ying texted another colleague, writing "I think some big media announcement is coming about us" and "I think it might be bad."
- On August 30, 2017, the Global CIO and Equifax's counsel told Ying about the breach and instructed him not to trade on that information. Ying did not disclose that he had exercised his stock options.
- After the close on September 7, 2017, Equifax publicly disclosed the data breach. The following day, Equifax's stock price dropped. Had Ying waited to sell his shares until after the breach was made public, he would have earned $117,000 less on the sale.
- Following an internal investigation several months later, the CIO's conduct was discovered, and he was asked to resign.

The SEC Complaint charged Ying with violations of Rule 10b-5 under the Securities Exchange Act of 1934 (Exchange Act) and Section 17(a) of the Securities Act of 1933 (Securities Act). The indictment charged Ying with securities fraud under Rule 10b-5 and securities and commodities fraud under 18 U.S.C. § 1348.[3] The elements of proof under both counts in the indictment are identical, and both are based on the same alleged activity. In an interesting twist, Ying's indictment represents the first instance in which prosecutors charged a defendant with classical insider trading (*i.e.,* trading oneself on inside information one obtained) under both Section 1348 and Section 10(b). (According to Ying's brief, "[t]he few cases where insider trading was charged under Section 1348 were not based on classical insider trading, but instead tipper/tippee or misappropriation liability.")

## Ying's Argument: What Material Nonpublic Information?

On June 11, 2018, Ying moved to dismiss the criminal indictment. He did not dispute the facts above. Instead, he argued that the indictment failed to allege that he knew or used any material nonpublic information when he exercised his stock options. Ying pointed out that the indictment

"describes little more than an employee who exercised options after being lied to by Equifax about the 'material nonpublic information' at issue." The indictment conceded that Equifax deliberately kept Ying in the dark about the breach. Ying argued that the prosecution had failed to identify any material nonpublic information he supposedly possessed. Ying also pointed out that the results of the internet searches he performed showed that Experian's stock price increased rather than decreased at the time of its data breach. If anything, Ying argued, the facts alleged in the indictment demonstrated that he did not know any material nonpublic information, and pointed to the same text messages that revealed Ying had not reached any conclusions, but was only putting "2 and 2 together." Ying drew a line between actual knowledge of inside information, and belief in the accuracy of hypothetical inside information. This, Ying argued, was not material nonpublic information, but mere speculation, at best.

Ying also argued that, at a minimum, one of the counts in the indictment should be dismissed as multiplicitous because it failed the *Blockburger* test. Under *Blockburger v. United States*,[4]

> when a single, completed criminal transaction violates two or more criminal statutes, the Double Jeopardy Clause does not shield a defendant against prosecution under one or more of the applicable statutes so long as "each statute requires proof of an additional fact which the other does not . . . ."[5]

## Motion Denied: "2 and 2" = Inside Information

On September 17, 2018, the magistrate presiding in Ying's case issued a report and recommendation (Report) that Ying's motion be denied. The Report found that the indictment sufficiently identified the material nonpublic information as the Equifax data breach, and further, that the indictment alleged that Ying "inferred [the breach] from the information he did receive from Equifax." Notably, this "inference" language is not in the indictment, though it does appear in the government's opposition brief. The Report dismissed Ying's argument that the indictment's lack of the word "used" was fatal, finding that the allegation that Ying "traded on the basis of material nonpublic information" sufficiently conveyed the elements of the crimes alleged. The Report did not reference the results of Ying's internet searches, though it did appear to count the fact of the searches as evidence of Ying's "inference" of a breach.

The Report also denied Ying's argument that the indictment was multiplicitous. Instead, the Report notes,

> although the evidence may be the same to prove the violations asserted in each count, . . . the focus is on the statutory elements of the offense, not the specific facts presented by the government to prove the offense.

The Report observed that securities fraud under Section 10(b) does not have a money or property element, while securities fraud under Section 1348 does.

## What It All Means

Ying's case stands out for several reasons. First, Ying is facing civil and criminal liability not for trading on information he misappropriated or was given in confidence, but for independently concluding his employer was the victim of a breach. While courts have upheld insider trading convictions for individuals who suspected they were in possession of inside information, those cases involved instances where the insider was given explicit information about the pending transaction.[6] In Ying's case, Equifax deliberately misled him and gave him false information. The charges asserted against Ying indicate that the SEC and DOJ are applying an extraordinarily broad interpretation of the insider trading knowledge requirement.

Under Rule 10b5-1, a trade is

> made "on the basis of" material non-public information . . . if the person making the purchase or sale was aware of the material nonpublic information when the person made the purchase or sale.

Here, if the material nonpublic information is the fact that Equifax was breached, Ying is facing incarceration and substantial monetary penalties for basically following his nose to what later proved to be the right conclusion.

*Even careful planning cannot prevent inadvertent discovery of material non-public information.*

Granted, the indictment lacks some of the additional details regarding Ying's correspondence at the time he was speculating about the breach that were included in the SEC complaint. However, even these details do nothing more than invite further speculation as to whether Ying had guessed that Equifax was the victim of the breach. Even if there were definitive proof that Ying had concluded that Equifax was the victim of the breach, allowing his guess (albeit a correct one) to stand in for his actual knowledge would be a significant expansion of the knowledge requirement for insider trading claims.

Second, Ying's indictment is a test of whether courts will permit dual insider trading claims brought under both Rule 10b-5(1) and 18 U.S.C. § 1348 to go forward when the claims are based on identical facts. While this would not change the government's pleading burden, it could significantly increase the scope of the defendant's potential liability. It remains to be seen whether the Report will be adopted, but at least for now, chances look grimmer for defendants.

Finally, the case illustrates the importance of developing a robust and flexible incident response plan, including processes for issuing trading blackouts during investigation of a breach, and how and when to communicate with employees who are not part the core incident response team. As Ying's case demonstrates, even careful planning cannot prevent inadvertent discovery of material non-public information.

## Practice Tips

Corporations should consider updating their cyber incident response plans to include provisions for issuing trading blackouts. The provisions should cover when to issue the blackouts, which employees and/or directors should be subject to the blackouts and for how long, and how they will be notified of the blackout. The response plan should also have a means of monitoring and enforcing the blackout.

Companies should consider establishing notification requirements from the company's sponsored stock plan administrator or custodian whenever employees exercise stock options.

Finally, corporate insider trading policies should address instances in which employees may obtain (whether directly or indirectly) non-public information regarding a potential data breach impacting the company or its customers and offer training to help employees identify when they might be in possession of material non-public information – and what they can and cannot do with that information.

### Notes

1. SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746, 17 C.F.R. §§ 229, 249 (Feb. 26, 2018) (*available at https://www.sec.gov/rules/interp/2018/33-10459.pdf*).
2. Complaint, SEC v. Ying, No. 18-1069, N.D. Ga. (Mar. 14, 2018).
3. Enacted in 2002 as part of the Sarbanes-Oxley Act, 18 U.S.C. § 1348 is patterned after the mail and wire fraud statutes and makes it a crime to obtain "by means of false or fraudulent pretenses, representations, or promises, any money or property in connection with the purchase or sale" of a security. A violation of Section 1348

carries a maximum prison sentence of 25 years. In contrast, a conviction of securities fraud under Section 10(b) carries a maximum 20-year sentence.

4. Blockburger v. United States, 284 U.S. 299, 304 (1932).
5. United States v. Williams, 527 F.3d 1235, 1240 (11th Cir. 2008).
6. *See* U.S. v. Mylett, 97 F. 3d 663 (2d Cir. 1996) (tippee was informed that tipper's employer was going to try to acquire corporate acquisition target); SEC v. Materia, 745 F. 2d 197 (2d Cir. 1984) (employee at financial printing firm given documents from which he could determine targets of proposed tender offers).