New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 259—NO. 92
MONDAY, MAY 14, 2018

White-Collar Crime

Expert Analysis

Insider Trading, or Trading by an Insider?

By **Elkan Abramowitz**

And **Jonathan Sack**

Employees of public companies routinely have confidential information about the businesses of their employers. As part of their jobs, people learn of major corporate events, such as mergers, but also less momentous but still important developments within a company, such as whether new products are flying off the shelves or sitting in warehouses. All or some of this information might be regarded as "material" under federal securities laws. Opportunities to engage in insider trading are thus not uncommon, especially since public companies routinely compensate employees (at least in part) with shares of stock or options to buy stock.

Companies have developed practices to reduce the risk of insider trading. Company codes of conduct and employee manuals routinely prohibit such trading. Beyond written policies, sensitive information is limited to small groups of core personnel, and information technology (IT) systems typically reduce the opportunities to gather secret information. For the most sensitive information, companies impose special trading "blackout" periods and inform affected staff that they may not trade in the company's securities during a specified period.

The inherent risk that an employee will trade on nonpublic information is illustrated by recent charges brought against an Equifax employee, Jun Ying, formerly Chief Information Officer of an Equifax business unit. In March, the SEC charged Ying with insider trading for selling Equifax stock in late August 2017—shortly before Equifax publicly announced a data breach that affected about 143 million consumers. In addition, a grand jury in the Northern District of Georgia returned an indictment which also charged Ying with insider trading.

> The charges raise interesting questions as to when nonpublic information within a public company should be deemed material for purposes of insider trading enforcement.

What stands out about the Ying charges is that he was "not told that Equifax had been breached." Rather, from what he saw and heard inside the company, Ying "conclude[d]," as the SEC put it, that Equifax had been breached. In an email that encapsulates the case, Ying wrote the following to one of his direct reports three days before his trading: "Sounds bad. We may be the one breached … . Starting to put 2 and 2 together."

After summarizing the allegations in the detailed SEC complaint (*SEC v. Ying*, No. 1:18-cv-01069-CAP (N.D. Ga. March 14, 2018), ECF No. 1), we discuss the implications of charging Ying with insider trading. The charges raise interesting questions as to when nonpublic information within a public company should be deemed material for purposes of insider trading enforcement.

The Allegations Against Ying

In August 2017, Equifax discovered a major breach of its IT systems which exposed personal data about millions of consumers. The company created a "crisis action team," consisting of security, legal and IT personnel, to deal with the breach and related issues, which was given a code name, "Project Sierra." Members of the Project Sierra team were told that information relating to the project "was confidential and should not be shared with anyone outside of Equifax's crisis action team." They were forbidden

ELKAN ABRAMOWITZ *and* JONATHAN SACK *are members of Morvillo Abramowitz Grand Iason & Anello P.C. Mr. Abramowitz is a former chief of the criminal division in the U.S. Attorney's Office for the Southern District of New York. Mr. Sack is a former chief of the criminal division in the U.S. Attorney's Office for the Eastern District of New York.* KEFIRA WILDERMAN, *an attorney, contributed to this article.*

to trade in Equifax stock, and Equifax instituted "a special trading blackout period for employees working on Project Sierra."

After determining that the breach was very serious, Equifax created a separate "notification and remediation plan for the millions of consumers affected by the breach," which was code named "Project Sparta." Project Sparta was kept separate from Project Sierra, and virtually all of the employees working on Project Sparta were not told of the breach and were not given specific instructions about the need for confidentiality. To the contrary, Equifax purposely misinformed the Project Sparta team, telling them that they were working to remediate a large data breach "for an unnamed client."

On a Friday afternoon (August 25), as part of Project Sparta, Ying and other IT personnel received an email that sought their assistance with remediation efforts that involved an "extremely time sensitive" unspecified "**VERY** large breach opportunity." (emphasis in original). Ying initially resisted accepting the assignment. On a one-minute call with the global Chief Information Officer (CIO), Ying was told that he was "expected to comply with the request" and that, at some point, he would understand what was happening.

It was around this time that Ying apparently began to infer—contrary to what he was being told—that the massive data breach was at Equifax, not an unspecified client. Immediately after the call with Equifax's global CIO, Ying wrote the email that will no doubt be a centerpiece of the litigation: "On the phone with [global CIO]. Sounds bad. We may be the one breached … . *Starting to put 2 and 2 together*." (Emphasis added.) Moments later, Ying responded to a text from Project Sparta's leader asking if he had any questions, as follows: "No question right now. Actually, I don't want to know ;) I told the team to [rally]."

Additional developments on Friday (August 25) seemed to confirm Ying's hunch that Equifax, not a client, had suffered the data breach. Communications with the global CIO and a direct report to Ying suggested that the remediation effort would be "highly unusual" and resemble Equifax's "Crisis Management Plan" for responding to a breach of Equifax's data systems. In addition, Ying learned that executives in Equifax's IT, Legal and Security departments were cancelling travel plans and unrelated meetings with Equifax clients. In an email to another employee regarding the cancellations, Ying wrote, "I think you now know why," adding that the cancellations were "related to all the mad scrambling … ."

> The charges against Ying may raise issues as to when and how broadly to impose trading blackouts.

By Monday morning (August 28), Ying was thinking about the possible impact of a large-scale data breach on Equifax stock options he had been granted as part of his compensation. Ying used his computer at work to search for information about the impact of a 2015 cybersecurity breach at another credit bureau, Experian. One hour later, Ying accessed his company-sponsored stock plan and exercised all of his 6,815 options to buy Equifax stock, which he then immediately sold for more than $950,000 in gross proceeds.

Two days later (August 30), Ying was notified that Equifax had been breached, and he became part of the Project Sierra team. Ying met for the first time with an attorney for Equifax, who told Ying that information about the breach could not be shared with anyone and that Ying should not trade in Equifax securities. Ying did not mention that he had already sold his Equifax stock two days earlier.

On September 7, Equifax announced the cybersecurity breach and revealed that about 143 million consumers in the United States may have been affected. The price of Equifax stock dropped almost 14 percent the next day on very high trading volume. In the SEC's analysis, Ying avoided more than $117,000 in losses by exercising his options and selling his stock prior to the public announcement. Following the announcement, Equifax conducted an internal investigation and learned of Ying's trading and determined that he should be fired because he had violated the company's insider trading policy. Ying was allowed to resign.

On March 14, 2018, the SEC charged Ying with violating §10(b) of the Securities Exchange Act and §17(a) of the Securities Act for trading in Equifax securities while in possession of material nonpublic information. In addition, an indictment was returned by a grand jury which charged Ying with two counts of insider trading in violation of §10(b) of the Securities Exchange Act and §1348 of Title 18.

The Materiality Issue

The defense will most likely center on the question of "materiality": whether the separate pieces of nonpublic information Ying received, which led him to "put 2 and 2 together," meet the "reasonable investor" test for materiality under federal securities laws. See, e.g., *United States v. Contorinis,* 692 F.3d 136, 143 (2d Cir. 2012). In this regard, the phrasing used in the SEC complaint is noteworthy. The SEC consistently uses the word "conclude" to describe Ying's belief that Equifax had been breached. A more neutral term would have been "infer," and

the defense may want to say that Ying was simply "guessing" about what had happened—especially since Equifax and its lawyers were acutely sensitive to who at Equifax had material information (and imposed a trading blackout) but did not impose a blackout on Ying until after the trading at issue.

Two insider trading cases shed light on when drawing inferences from multiple pieces of information violates the securities laws. In 1996, the Second Circuit upheld the criminal conviction of a defendant who was tipped by a friend who suspected that an acquisition by his employer (AT&T) was imminent. *United States v. Mylett*, 97 F.3d 663 (2d Cir. 1996). A supervisor brought to the tipper's attention a Wall Street Journal article which reported that AT&T and NCR Corporation were discussing ways to integrate their businesses. The supervisor cautioned the tipper not to discuss with anyone what was in the article. The tipper also had been asked to conduct a feasibility study relating to a merger between AT&T and an unnamed company with the "same vital statistics" as NCR.

On appeal, the defendant argued that the tipper's information was not material and non-public in light of the publicly available information. The court held that the information conveyed by the tipper was "substantially more specific than that in the newspaper" and had put the facts in the newspaper in "their proper context." Id. at 666-67. The tipper's information was material in that it "conveyed information that indicated a much higher level of probability than was publicly available concerning an event of great magnitude in the corporate life" of the tipper's company. Id. at 667-68.

In *SEC v. Steffes*, No. 10-CV-6266 (N.D. Ill. Sept. 20, 2010), the SEC charged two railroad employees and their families with insider trading. According to the SEC, one of the employees, the Vice President and Chief Mechanical Officer, became aware of the pending acquisition of the railroad's parent company when, for the first time, the parent's Chief Financial Officer requested a list of the company's locomotives, freight cars, trailers and containers and their corresponding values. He also observed an unusual number of investment bankers touring the railroad yards. His nephew, the other employee defendant, was a trainman who also observed an unusual number of tours by people in business attire. The district court denied a motion to dismiss, holding that "it is well established that a defendant can be held liable for insider trading when he or she obtains and acts on pieces of information, which, 'piece[d] together,' constitute material nonpublic information." *SEC v. Steffes*, 805 F. Supp. 2d 601, 610 (N.D. Ill. 2011).

The government's case in *Steffes* touches on what has come to be called the "mosaic theory." Under this theory, people evaluate a security's value and investment potential based on multiple discrete pieces of information that form a mosaic; while each piece is not material in isolation, adding the pieces together may give rise to material information. The theory has generally been invoked as a defense to insider trading charges, for example, when a securities analyst argues that a bit of nonpublic information was not in itself material, but contributed to a purchase or sale decision in combination with publicly available information. In a case such as *Steffes*, or *Ying*, the government would be accepting that decisions are made based on multiple pieces of information but then use the mosaic concept affirmatively to explain how individual pieces of nonpublic information collectively became material.

The mosaic concept may very well be fleshed out as the *Ying* cases proceed. Of note for the defense, four of the *Steffes* defendants went to trial and were found not liable after a nine-day jury trial. Two defendants settled with the SEC without admitting or denying the allegations.

Conclusion

The charges against Ying may raise issues as to when and how broadly to impose trading blackouts. Equifax concluded that it would suffice to restrict trading by employees who were expressly told of the company's massive data breach. But the charges against Ying suggest that the blackout should perhaps have been broader and designed to include individuals who could draw inferences from access to more limited information. Of course, overly broad blackouts carry their own dangers—such as informing larger numbers of people that something significant, even if not identified, is occurring—and these risks will have to be weighed against the risks of too narrow blackouts.

The charges against Ying also invite consideration of whether a meaningful difference remains between civil and criminal enforcement decisions when it comes to insider trading. In this case, one could argue that the materiality issues are sufficiently debatable that enforcement should be left to civil charges by the SEC. But federal criminal charges were filed and will almost certainly be litigated before the SEC charges, exposing Ying to two separate proceedings. Perhaps defense attorneys need to accept that in all but the most borderline cases—because the proof is so thin or the trading and profits so small—an indictment will be sought alongside civil charges.