LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, JULY 11, 2018

New lessons about data breaches and insider trading

By Joshua M. Robbins and Adam M. Sechooler

The massive Equifax data breach has brought new attention to the challenges companies face in securing consumers' personal information. The July 2017 incident exposed the sensitive personal information of 143 million Americans. It also caused the price of Equifax's shares to drop substantially. New laws intended to hold companies accountable for protecting sensitive information may raise the stakes when data breaches occur. Combined with growing awareness of data breaches by shareholders and consumers, and increasingly aggressive breach-related litigation, data breaches may increasingly become material events for purposes of securities law. This, in turn, will trigger duties to disclose the information to investors and for insiders possessing non-public information to refrain from trading. And when those rules are inevitably violated, it will create opportunities for the Securities and Exchange Commission and Department of Justice to step in.

While the potential for data breach-related insider trading may be growing, significant questions remain. Critically, the elements of materiality and scienter can be even more difficult for the government to prove in a data breach-related case compared to other insider trading scenarios. The impact that a given breach incident will have on share prices is unpredictable, and may depend on the type of company involved and — more importantly — the nature and scope of the breach. Additionally, the full extent of a breach is often not immediately apparent; it may take days, weeks or months to confirm. Further, information about a breach may not be shared fully within the company, even among those charged with fixing it. Thus, proving that an individual officer or employee knew that he or she possessed material non-public information regarding a breach at a specific time can be daunting even for experienced investigators.

New York Times News Service
The offices of Equifax, the consumer credit reporting agency, in Atlanta, Sept. 12, 2017.

How is the government responding to these challenges? The SEC's formal guidance on public company cybersecurity disclosures, issued earlier this year, is not very revealing — stating broadly that insiders should be "mindful of complying with the laws related to insider trading in connection with information about cybersecurity risks and incidents, including vulnerabilities and breaches," while encouraging companies to consider restricting insiders' trading in their securities while investigating a cybersecurity incident. But a series of recent prosecutions and enforcement actions stemming from the Equifax breach are more telling, and portend an aggressive approach.

Equifax learned about suspicious network activity in July 2017, and shortly thereafter discovered that massive amounts of consumer data had been exposed. In response, it created two teams to work on a fix. For one team ("Project Sierra"), Equifax instituted a special trading blackout period. The other team ("Project Sparta") was not told that Equifax was the victim of the breach. Rather, to limit the number of people who knew that Equifax had been breached, the members of Project Sparta were told that they were working for an Equifax client that had experienced a large data breach.

The prosecutions concern two members of Project Sparta, the team that was subject to the ruse by Equifax management and was not under a trading blackout. Jun Ying, the former chief information officer of one of Equifax's divisions, was expressly told that the breach involved a company other than Equifax itself, but allegedly deduced that this was untrue, texting a colleague that "[w]e may be the one breached" and that he was "starting to put 2 and 2 together." After conducting an internet search regarding the effect an earlier breach had on the share price of Equifax's competitor, Experian, Ying exercised all his options in Equifax shares and sold them, before the breach was disclosed. Separately, software development manager Sudhakar Reddy Bonthu, who was also told the breach concerned a different company, allegedly received a dataset file whose name included the terms "EFX" (Equifax's stock symbol) and "Databreach." He then purchased put options in company stock via an account in his wife's name. The government alleges that Bonthu told a colleague he had "figured out" that Equifax was the victim of the breach before the Equifax breach was publicly disclosed.

Both Ying and Bonthu face civil and criminal charges for insider trading; Ying was charged in March and Bonthu late last month. While Bonthu waived indictment, suggesting that he may plead guilty, Ying is fighting the charges. In a motion to dismiss the indictment, Ying raises precisely the issues — materiality, knowledge and intent — that will likely present challenges for the government in breach-related insider trading cases. In particular, Ying notes that, as the government admits, his company lied to him, falsely telling him that it was not the entity that had suffered the breach at issue. Even if he suspected that his superiors were misleading him, he argues, how can that amount to knowledge that the breach impacted Equifax itself? While Bonthu has not as yet filed a similar challenge, he could presumably raise the same point; indeed, the charging documents include fewer details regarding how he deduced that

Equifax was the breach victim. Importantly, however, speculative information can nonetheless be material if it would be important to investment decisions.

Both defendants could also conceivably raise another point: Absent evidence that they were told of the full scale of the breach, how could they have known that it would likely impact Equifax's share price, and thus that the information was material? The SEC's complaint against Ying alleges that he was given information on the number of consumers potentially affected and the involvement of Equifax's senior management, and that he made several statements indicating that he understood that the issue was serious. But the government does not claim that Ying was given the full picture of the breach before he traded. And in his motion, Ying argues that his internet research on Experian actually showed that its share price rose after its breach was disclosed. The charging documents on Bonthu are even thinner on this issue, providing no specifics on what he learned about the breadth or impact of the breach. Presumably, the government is relying heavily on his anomalous trading activity — he had never before traded in Equifax options — as circumstantial evidence that he knew the information was significant.

The fates of Ying and Bonthu aside, their cases also highlight the difficult choices companies face when data breaches are unfolding and have not yet been disclosed. Equifax's decision to reveal the breach to only a subset of "need-to-know" insiders while giving disinformation to others involved in the response is perhaps understandable. A company in that situation may not want to risk a panic among employees, a chaotic and premature disclosure, and the possibility of inviting outsiders to exploit the breach before it has been remedied, and thus may concoct a ruse to control the flow of information in the interim. As these cases demonstrate, it may also want to use this tactic to discourage insider trading among employees. However, deliberately misleading one's own employees, even for legitimate reasons, is fraught with its own risks. For example, what if the employees spread the false information outside the company, including to the investing or consuming public? Would the company be held responsible? At a minimum, the approach may provide a defense to employees looking to trade on the breach, who may reason that they cannot be considered "insiders" when they are kept out of the loop.

But if the Equifax cases are any indication, the DOJ and the SEC do not appear overly concerned. Given the explosion of data breaches and their potentially increasing effect on share prices, the government is understandably keeping a careful watch on the potential for insider trading in their wake. If prosecutors are willing to look beyond the challenges of proving materiality and intent even in cases involving low-level executives whose company misled them about the breach at issue, they will presumably have little hesitation in pursuing such charges in other situations. Insiders, including the non-traditional sort, should take note.

Joshua M. Robbins *is a partner and* **Adam M. Sechooler** *an associate at Greenberg Gross LLP. Mr. Robbins chairs the firm's White Collar Defense and Government Investigations practice.*


ROBBINS


SECHOOLER