LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

THURSDAY, OCTOBER 19, 2017

PERSPECTIVE

Growing risk of insider trading on data breaches

By Joshua M. Robbins
and Adam M. Sechooler

The recent Equifax hack exposed sensitive personal information of 143 million Americans. Shortly after the hack, the SEC and Department of Justice opened insider trading investigations based on allegations that Equifax's CFO and other senior executives sold $1.8 million of shares in the company before the breach was announced. Although this is one of the first such episodes, it will not be the last, as changes in business practices and developing privacy law may mean that more companies will see share prices fall in the wake of cybersecurity incidents, while the government increasingly scrutinizes how those companies and their officials respond. The unique nature of data breach incidents and the lack of clear legal guidance make this a challenging area for companies and regulators alike.

The Equifax breach illustrates two overwhelming and related trends: companies' systematic collection of consumers' personal information and hackers' theft of that information. While companies like Facebook have long relied on user data for their business platforms, the phenomenon is now spreading across the entire economy. Existing companies in various sectors use apps, big data processing and other means to track and analyze customer data, employing it for product development and marketing purposes. As new consumer technologies such as fitness trackers, "smart" appliances and self-driving cars incorporate this model, firms' possession of sensitive personal information is an inescapable feature of the new digital economy.

The risks of that model are equally clear. The customer data companies collect has enticed malicious cyber actors lurking across the internet. State-sponsored groups, organized crime syndicates, and others have generated a steady stream of high-profile corporate data security breaches. And the torrent shows no signs of abating.

New York Times

Richard Smith, the former chief executive of Equifax, arrives to testify before the House Energy and Commerce Committee in Washington, Oct. 3.

Historically, Little Share Impact = Little Enforcement

An insider trading violation under the Securities Exchange Act of 1934 and SEC Rule 10b-5 requires, among other things, that the information traded on be "material" — that is, that a reasonable investor would view the information as significant in deciding whether to trade. It also requires that the defendant act with scienter — an intent to deceive or defraud.

These elements have been difficult to meet in most data breach cases. Even when the breaches have been massive, affected companies have generally not seen corresponding share price declines. For example, after Home Depot disclosed in 2014 that 56 million of its customers' credit cards had been compromised, its shares declined only slightly, and soon after returned to near their all-time high. Other large breaches at Kmart/Sears, Sony and JP Morgan Chase followed similar patterns.

As a result, the materiality of data breaches to company share prices has been so unclear that even private shareholder lawsuits in the wake of such events have been relatively scarce. The SEC and DOJ have been even less likely to scrutinize trading patterns in such cases, as there was little apparent opportunity to profit from early access to word of a breach.

Rising Costs of Breaches

But that may be changing, as the costs of breaches to the affected companies are becoming larger and slightly more predictable. Litigation filed against companies by customers and financial institutions whose information has been stolen has led to a number of court decisions finding companies potentially liable for failing to adequately safeguard that data. For example, various federal appellate courts have reached decisions favorable to data breach plaintiffs, while Target settled claims by credit card issuers in its breach case for some $100 million. At the same time, state and federal regulators — such as the Federal Trade Commission and state attorneys general — have been cracking down on companies for their cybersecurity failings.

There are other costs as well. Companies hit by hackers suffer reputational harm that may impact sales. This is particularly true for companies that depend on consumers' trust and collect personal information as part of the basic customer experience. In addition, the costs of remedying security breaches and complying with increased regulatory requirements can add up. Target recently estimated that its total costs from its 2014 breach exceeded $200 million. Further, even when hackers do not access customer information, they may take intellectual property critical to a company's market advantage.

Data Breaches as Material Events

These developments mean that data breaches may increasingly be viewed as material to share prices. Growing legal, financial and commercial costs mean that a company's disclosure of a breach is more likely to result in a sharp drop in the price of its shares. Equifax saw its shares fall some 18 percent in the days following its revelation of the hack. After it disclosed its own massive data breaches, Yahoo was forced to trim $350 million off the price of the sale of its operating business to Verizon.

While these have been outliers compared to other companies suffering earlier breaches, they may soon have company.

The increasing materiality of data breaches means that they are more likely to implicate company insiders' duties to refrain from trading. As a result, breach incidents will draw increasing scrutiny from securities regulators. While neither the SEC nor the DOJ have filed an enforcement action resulting from a data breach, the SEC's leaders have made clear that it is more than ready to do so in the appropriate case.

These do not appear to be empty threats, as shown by the SEC and DOJ investigations into possible insider trading by Equifax executives in the days after the breach was discovered. Were the agency to uncover evidence that the executives knew of the breach and its seriousness at the time they sold, which was before the breach had been publicly disclosed, it could well result in both civil and criminal prosecution.

Complexities of Breach-Related Disclosure Investigations

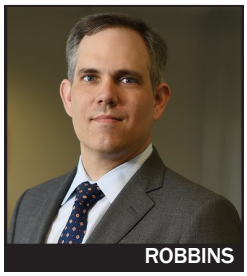
The nature of data breaches, however, creates challenges both for executives deciding whether to trade and for prosecutors investigating an incident. In particular, materiality can be quite difficult to determine at the outset of a breach. A typical large company is hit with numerous hacking attempts every day, and a number of them may succeed in evading certain security measures or inflicting limited damage. That is quite different from the massive and devastating thefts that have resulted in headlines over the past several years. Even IT or security personnel, let alone finance or legal executives, may not know whether a breach is major or minor until sometime after an issue is first discovered. As a result, it can be difficult to prove that the insider had the requisite knowledge or acted with scienter at the time of the trade.

For example, according to congressional testimony from Equifax's former CEO Richard Smith, company security personnel first observed the suspicious activity that turned out to be the breach on July 29, and Smith was notified two days later. But it was not until mid-August — more than a week after the share sales under investigation — that company personnel determined that a large volume of individuals' personal information might be compromised. If this timeline holds true, it may prove impossible to show that the executives involved had any sense of the materiality of the issue at the relevant time. That could thwart any 10b-5 prosecution even if, contrary to Equifax's statements, the executives knew about the initial security intrusion.

This technical nuance is compounded by the rapidly changing law on breach liability, as discussed above, and by the fact that different types of companies may face different degrees of fallout among customers and others in the face of a breach. Even if it could prove that an executive knew, before selling shares, that a breach was largescale and affected customer data, the executive could argue that he did not know, based on prior cases, that disclosure of the breach would cause share prices to fall. But as data breach law continues to evolve, and as more cases like Equifax and Yahoo emerge, that argument may prove increasingly difficult to make.

Joshua M. Robbins *is a partner at high-stakes business litigation law firm Greenberg Gross LLP and chair of its White Collar Defense and Government Investigations Department. He can be reached at jrobbins@ggtriallaw. com or (949) 383-2840.*

Adam M. Sechooler *is an associate with the firm, and can be reached at asechooler@ggtriallaw.com or (949) 383-2815.*


ROBBINS


SECHOOLER

Reprinted with permission from the ***Daily Journal***. ©2017 Daily Journal Corporation. All rights reserved. Reprinted by ReprintPros 949-702-5390.