riskINSIGHTS
FALL 2017

Equifax Data Breach Litigation includes a Securities Suit

In the wake of credit monitoring and reporting firm Equifax's recent announcement that it had sustained a data breach involving 143 million U.S. customers, a wave of consumer class action lawsuits have followed. In addition, the litigation wave included at least one securities class action lawsuit; with more securities suits likely to follow. Although data breach-related D&O claims have not fared particularly well in the past, there are features of the Equifax situation that may put the securities suits against Equifax in a different category. An interesting question is the extent to which the new lawsuit portends further data breach-related securities litigation going forward.

BACKGROUND

On September 7, 2017, Equifax announced a "cybersecurity incident" potentially impacting 143 million U.S. customers. The company's press release stated that during the period from mid-May through July 2017, criminals had exploited a U.S. website vulnerability to gain access to customer information. The company discovered the breach on July 29, 2017. The information includes names, Social Security numbers, birth dates, addresses, and in some instances, driver's license numbers. The credit card numbers of about 209,000 U.S. consumers were also breached. Upon discovering the breach, the company launched a forensic review to determine the scope of the breach. The company also notified law enforcement officials.

RT ProExec
Setting New Expectations

CONNER STRONG & BUCKELEW
INSURANCE | RISK MANAGEMENT
EMPLOYEE BENEFITS

On September 11, 2017, *USA Today* reported that at least 23 proposed consumer class action lawsuits had already been filed, adding that "additional cases are likely to come."

Later in the day on September 7, 2017, Bloomberg reported that the company's SEC filings showed that on August 1, 2017 – that is, just days after the company discovered the data breach — Chief Financial Officer John Gamble sold shares worth $946,374 and Joseph Loughran, president of U.S. information solutions, exercised options to dispose of stock worth $584,099. Rodolfo Ploder, president of workforce solutions, sold $250,458 of stock on Aug. 2. None of the filings lists the transactions as being part of 10b5-1 trading plans. The company later issued a statement saying that none of these officials were aware of the data breach at the time they sold their shares, which in each case represented only a small percentage of their holdings.

THE EQUIFAX CONSUMER LITIGATION

On September 11, 2017, *USA Today* reported that at least 23 proposed consumer class action lawsuits had already been filed, adding that "additional cases are likely to come." The newspaper noted that the number of cases and the speed with which they were filed "show an eagerness by plaintiffs' law firms to stake swift claims on behalf of consumers who eventually might be in line for a share of either a court judgment against Equifax or a settlement by the company."

Among other things, the consumer lawsuits allege security negligence by Equifax, as well as the company's delay in alerting the public. The lawsuits also refer to smaller data breaches the company sustained in 2013, 2016, and earlier in 2017. According to one of these lawsuits, the company "knew and should have known of the inadequacy of its own data security."

THE EQUIFAX SECURITIES LITIGATION

Along with the consumer lawsuits, the avalanche of litigation that followed Equifax's data breach announcement now includes at least one securities class action lawsuit. Just as USA Today said with respect to the consumer lawsuits, with respect to the securities lawsuits as well, more are likely to follow.

Plaintiffs' lawyers announced in a September 11, 2017 press release that they had filed a securities class action lawsuit in the Northern District of Georgia against certain executive officers and directors on behalf of a plaintiff shareholder. According to the press release, the complaint alleges that the defendants issued materially false or misleading statements or failed to disclose that "(1) the Company failed to maintain adequate measures to protect its data system; (2) the Company failed to maintain adequate monitoring systems to detect security breaches; (3) the Company failed to maintain proper security systems, controls and monitoring systems in place; and (4) as a result of the foregoing the Company's financial statements were materially false and misleading at all relevant times."

The complaint purports to be filed on behalf of all Equifax shareholders who purchased company shares between February 25, 2016 and September 7, 2017. The complaint names as defendants, in addition to the company itself, the company's Chairman and CEO, Richard F. Smith, and its CFO, John W. Gamble, Jr. The complaint specifically references the trading in company shares by Gamble and other company executives. The complaint also references a variety of alleged statements by the company during the

class period relating to the quality of its data protection and security measures. The complaint alleges that on the news of the company's data breach the company's shares fell nearly 17%.

DISCUSSION

Although observers have long been predicting that we would see significant amounts of data breach related D&O litigation, at least up to this point the litigation has never really materialized.

Among the most significant reasons that we have not seen much data breach related securities class action litigation is that companies' share prices have not reacted significantly to the companies' announcements that they had sustained a data breach. Without a significant stock price movement, the potential suits were unattractive to the plaintiffs' lawyers.

In the absence of a stock price drop that might support a securities class action lawsuit, the plaintiffs' lawyers have filed shareholder derivative suits, at least in the few instances where a data breach has led to a D&O claim. Data breach-related shareholder derivative lawsuits have fared particularly poorly, as these cases have generally been dismissed. The one exception is the Home Depot data breach-related shareholder derivative lawsuit. The Home Depot case was also dismissed but it eventually settled while the appeal of the dismissal was pending; the case settled for the company's agreement to pay about $1.1 million in plaintiffs' attorneys' fees.

The one recent exception to the generalization about the absence of data breach-related securities litigation is the securities class action lawsuit filed earlier this year relating to Yahoo!'s massive 2016 data breach. The Yahoo! lawsuits were filed after public announcements that because of the news about the data breach, Verizon's planned acquisition of the company was to be postponed and the terms renegotiated. The Yahoo! securities data breach-related securities class action lawsuit remains pending.

The recent Equifax securities class action lawsuit arguably represents the exceptional case where a company's share price declined significantly after the announcement of a data breach. The share price decline following Equifax's data breach announcement undoubtedly reflected the fact that the company's business model depends on maintaining the confidentiality of customers' sensitive financial information. The sheer magnitude of the breach was likely also a factor; although the Equifax breach is not the largest data breach to date, it may represent one of the highest profile breaches involving sensitive personal information.

The alleged insider trading may also make the Equifax case more attractive to prospective litigants. The company has claimed that the officials were not aware of the breach when they traded. In addition, the sales themselves are relatively small and reportedly only involve small portions of the officials' holdings. Nevertheless, the plaintiffs will likely try to argue that the officials sought to capture trading profits by trading in their shares before the news of the breach was publicly released.

The fact that the insider trading took place after the breach had been discovered, but before the breach was publicly disclosed, highlights the danger involved when a company delays publicly disclosing that it has sustained a cybersecurity incident. The company's press release states that the company delayed disclosing the breach while it conducted a forensic examination of the breach to determine its scope. In the wake of Equifax's data breach disclosure, one of the issues that will likely be examined in great depth is the question of how quickly companies should disclose information about a breach, particularly if the cause, scope, and seriousness of the breach is unknown when a company discovers that it has been hacked.

How the Equifax case ultimately will fare remains to be seen; in particular, whether the specifics of the plaintiffs' allegations are sufficient for the case to survive motions to dismiss. It probably should be added that there will undoubtedly be other securities complaints filed; additional lawsuits may contain additional allegations — including,

for example, reference to the supposed earlier data breaches the company had sustained.

Notwithstanding the lack of success plaintiffs have had with data breach-related shareholder derivative lawsuits, Equifax may seek to file derivative lawsuits against company officials as well. Further, several media reports have suggested that the SEC may be looking into insider trading issues.

The Equifax securities litigation will be interesting to follow. An even more interesting question is whether it portends further data breach-related securities class action litigation in the future. The fact that the company's share price reacted so significantly suggests the possibility that going forward at least some companies announcing a cybersecurity incident may also experience significant stock price movement, which in turn likely would lead to securities litigation. The Equifax lawsuit, and the Yahoo! data breach securities lawsuit before it, represents a specific and relatively new category of securities class action litigation. How many of these kinds of lawsuits will emerge is a question that has important implications for the companies and for their D&O insurers.

ABOUT THE AUTHOR

This article was prepared by Kevin M. LaCroix, Esq. of RT ProExec. Kevin has been advising clients concerning Directors' and Officers' Liability issues for nearly 30 years. Prior to joining RT ProExec, Kevin was President of Genesis Professional Liability Managers, a D&O Liability insurance underwriter. Kevin previously was a partner in the Washington, D.C. law firm of Ross Dixon & Bell.

Kevin is based in RT ProExec's Beachwood, Ohio office. Kevin's direct dial phone number is (216) 378-7817, and his email address is kevin.lacroix@rtspecialty.com.

ABOUT RT PROEXEC

RT ProExec is the Professional & Executive Liability Division of R-T Specialty, LLC. R-T Specialty, LLC is an independent wholesale insurance brokerage firm that provides Property, Casualty, Transportation and Professional & Executive Liability insurance solutions to retail brokers across the country. Our proven leadership, deep talent pool, and commitment to coverage and service has made us one of the largest wholesalers in the Professional & Executive Liability insurance marketplace.

ABOUT CONNER STRONG & BUCKELEW

Conner Strong & Buckelew is among America's largest insurance brokerage, risk management and employee benefits brokerage and consulting firms. The firm is an industry leader in providing high-risk businesses with comprehensive solutions to prevent losses, manage claims, and drive bottom line growth. Its employee benefits practice focuses on providing best-in-class benefits administration, health and wellness programs and strategic advisory services.

The company provides insurance and risk services to a wide-range of industries including but not limited to aviation, construction, education, healthcare, hospitality & gaming, life science & technology, public entity and real estate. Additionally, Conner Strong & Buckelew and its affiliates offer a number of innovative and specialty solutions which include captive strategies, construction wrap-ups, executive risk, safety and risk control, and private client services.

Founded in 1959 with offices in New York, New Jersey, Pennsylvania, Delaware and Florida, Conner Strong & Buckelew has a team of nearly 400 professionals, serving clients throughout the United States and abroad.

DISCLAIMER

CONNER STRONG & BUCKELEW

contact us

Terrence Tracy
Executive Vice President

Conner Strong & Buckelew
connerstrong.com | 267-702-1458