BEECHER CARLSON

EXAMINING THE IMPACT: D&O RISK DUE TO CYBER BREACHES

Cyber breaches have always hit companies' standalone cyber and property coverages in various ways. Until recently, D&O insurance has generally been shielded from the devastating effects of a breach; however, the massive securities class action and derivative settlements of Yahoo! and the current litigation against Equifax (and others) have changed this. A pattern of securities litigation resulting from the handling (or mishandling) of a data breach is currently emerging and becoming more prevalent.

Shareholders and the plaintiffs' bar have previously focused securities litigation on data breaches and the resulting effects on stock prices, which came in the form of derivative lawsuits based on alleged breaches of fiduciary duties. These suits were largely unsuccessful due to the high bar for prosecuting such lawsuits. Based on the current trend, however, shareholders have brought securities class action claims primarily based on alleged material misrepresentations to the market with respect to the adequacy or strength of the company's data security and monitoring systems as well as failure to timely disclose a data breach.

Yahoo!

In March 2018, Yahoo! agreed to an $80,000,000 settlement with shareholders in connection with two data breaches that affected more than one billion user accounts. This was the first significant securities class action settlement following a data breach and illustrated a potential avenue for shareholders to bring successful claims. In addition to the securities class action settlement, Yahoo! settled an accompanying derivative lawsuit for $29,000,000 in January 2019.

Following the announcements of the Yahoo! breach, the company's stock price fell, and the value of the company dropped in connection with its acquisition. This indicated a quantifiable loss to shareholders that had not been demonstrated as clearly in prior cases, which may have led to the ultimate settlement. Shareholders additionally asserted that they were unfairly disadvantaged by the untimeliness of Yahoo!'s disclosure of the data breach. This differed from prior cases that largely claimed the companies' statements prior to the data breach were materially false or misleading.

Equifax

Following the Yahoo! settlement, a ruling in the Equifax case demonstrated that these claims may be gaining some traction in the courts. On January 28, 2019, the court ruled that the securities class action against Equifax survived defendants' motion to dismiss, and the litigation is proceeding against the company and its Chief Executive Officer, Richard Smith. The lawsuit arises from an announcement in September 2017 stating that hackers had breached Equifax's consumer database and accessed millions of records containing personally identifiable information.

Shareholders allege that the company made multiple misleading statements and omissions about the adequacy of the company's cybersecurity, artificially inflating the company's share price and resulting in a loss of value when the data breach was revealed. It is worth noting that this breach has surfaced additional exposure concerns including downgraded rating outlooks based on cybersecurity issues. Following Equifax's announcement of a $700M settlement in connection with the data breach itself, the plaintiffs' bar will be watching this accompanying securities case closely for perspective on the probability of success in future data breach securities actions.

Numerous securities lawsuits against companies that have experienced a data breach are pending (including PayPal and FedEx), and their resolutions will continue to shed light on the severity of potential D&O liability faced by companies following data breaches. With a heightened focus on these lawsuits, it is important to bear in mind that the statements companies make about data security in their filings, press releases, and other communications are critical. In anticipation of these claims, companies must exercise best practices when representing the adequacy and accuracy of their cybersecurity and privacy systems and must remember that it is imperative to disclose any breaches in a timely manner. Working closely with your D&O and cyber insurance brokers is key to assessing the risk and insuring appropriately.

Jessica Slater is a claims advocate for Beecher Carlson's Executive Liability Practice in New York. She works in conjunction with client risk management teams to review all executive liability claim matters against applicable policies for coverage, submit notifications to insurance programs, and advocate on behalf of clients with the markets. Jessica is a recent graduate from the New York Law School. She can be reached via email at jslater@beechercarlson.com.