KING & SPALDING

Client Alert

Business Litigation Practice Group

February 21, 2013

Cybersecurity: The Next Big Wave in Securities Litigation?

News broke this week about significant cybersecurity breaches at many U.S. corporations that raises the possibility of a new wave of SEC enforcement actions, class actions, and derivative lawsuits. A front page New York Times article reported that cybersecurity firm Mondiant identified a Chinese military unit that hacked over 140 organizations over the last several years, stealing valuable intellectual property such as technology blueprints, proprietary manufacturing processes, business plans, and pricing documents. Companies affected by these attacks represent a wide range of industries, including information technology, construction, aerospace, and energy. The severity of these attacks will likely spur enforcement activity at the SEC, which has warned issuers about their cybersecurity disclosure obligations since 2011 in published disclosure guidance. The report and the likely reaction from the SEC will re-focus attention on cybersecurity controls and disclosure practices.

This startling report joins the growing chorus of politicians and commentators who are pushing for more attention to this significant economic threat. Just last week, President Obama signed an executive order calling for added cybersecurity to protect critical sectors of the economy, including banking, utilities, and transportation. As the scope and seriousness of cybersecurity threats become more widely understood, it is likely that this issue will continue to gain momentum among both government regulators and opportunistic plaintiff lawyers seeking to catch the next wave of shareholder litigation.

Breaches in a company's cybersecurity may result in a wide range of negative outcomes, including the loss of competitive advantage, decreased business abroad, a devaluation of intellectual property, increased expenditures on data security, and costly litigation. Because these data breaches may have an adverse impact on a company's financial performance, failure to disclose such events promptly may put a company at risk of facing formal SEC investigations, shareholder class actions, or derivative lawsuits. Accordingly, companies should be aware of the potential risks that they face from government regulators and private lawsuits when choosing whether or not to disclose breaches in their cybersecurity.

For more information, contact:

Paul R. Bessette
+1 512 457 2050
pbessette@kslaw.com

Michael J. Biles
+1 512 457 2051
mbiles@kslaw.com

King & Spalding
Austin
401 Congress Avenue
Suite 3200
Austin, Texas 78701
Tel: +1 512 457 2000
Fax: +1 512 457 2100

www.kslaw.com

The SEC's Position

The SEC has already taken a firm stance on cybersecurity disclosures, and clearly views this issue as ripe for enforcement actions. In late 2011, the SEC's Division of Corporation Finance published disclosure guidance relating to cybersecurity risks and incidents. These guidelines are not mandatory rules creating new disclosure requirements, but rather an explanation of how the SEC staff believes cybersecurity risks and incidents should be treated under current securities law. Specifically, the SEC believes that companies should disclose the risk of cyber incidents in a company's "risk factors" and that specific material cybersecurity breaches be disclosed in their Management Discussion and Analysis. Furthermore, they note that cybersecurity breaches may have a broad impact on a company's income and assets, and that these impacts should be reflected in a company's financial statements.

This guidance seems to have had a limited impact on corporate disclosure thus far, with the vast majority of companies that have been affected by hacking events choosing to keep these events confidential. While the SEC acknowledges in its guidance that corporations do not need to disclose details that would compromise their cybersecurity efforts, it insists that current disclosure requirements apply to the reporting of cybersecurity breaches. Given the increasing awareness of this hot issue, it is likely that the SEC will increase pressure on companies to disclose such events. If the SEC chooses to initiate formal investigations, then it may even use its subpoena power to gain detailed records of past cybersecurity breaches from third-party technology security companies.

If the SEC chooses to pursue formal actions against companies that have failed to disclose cybersecurity breaches, then it has at its disposal a wide range of options, including actions based on securities anti-fraud provisions such as Rule 10b-5. More likely, the SEC may try to establish books and records violations under Rule 13b2-2, which requires only simple negligence to establish liability. Given that the SEC's guidance has made it clear that cybersecurity breaches may require recognition of impaired assets and reductions in projected future cash flows, books and records violations seem to be the "low-hanging fruit" for SEC investigations into non-disclosure of cybersecurity breaches. Regardless of the specific method of enforcement that the SEC pursues, companies that have experienced significant cybersecurity breaches should prepare themselves for potential SEC investigations and lawsuits.

Securities Class Action Litigation

The most significant ingredient to a securities class action claim from the perspective of the plaintiff's securities class action bar is a significant stock drop in close proximity to a disclosure. This is important because it provides an essential link to causation, materiality, and damages—three essential elements to a securities fraud claim under Section 10(b) of the Exchange Act of 1934. Accordingly, a company that experiences a cybersecurity breach will likely not be a target of a securities class action unless the disclosure of the breach can be linked to a statistically significant drop in the company's stock price.

Despite the SEC's adamant position that cybersecurity issues are material to ordinary investors and warrant specific disclosures, recent news of cybersecurity breaches at several public companies have not resulted in meaningful stock drops for the companies at issue. For example, on February 19, 2013, Apple Computer admitted that it was a victim of several attacks by Chinese hackers. Although Reuters described Apple's disclosure as "an unprecedented admission

of a widespread cybersecurity breach," the stock market had a ho-hum reaction to the disclosure—Apple's stock price was essentially unchanged on February 19 (it opened at $461.10 per share and closed at $459.99).

In an efficient market[1], one would expect the disclosure of a cybersecurity breach—that has a measurable impact on a company's financial performance—to result in a meaningful drop in the Company's stock price. Because cybersecurity breaches are a relatively new phenomena, however, investors may not be able to measure how such events might impact the financial performance of companies. As investors become more knowledgeable about the risks and financial impacts of cybersecurity breaches, disclosures of these breaches may be more likely to impact stock prices and thus result in securities class action litigation.

Derivative Lawsuits

Another potential securities litigation risk for companies dealing with a cybersecurity breach is shareholder derivative litigation against officers and directors. Shareholders might allege, for example, that the directors of a company that experienced a cybersecurity breach breached their fiduciary duties to the company by failing to ensure adequate security measures. These so-called *Caremark*[2] claims require shareholders to demonstrate 1) that the directors knew or should have known that violations of the law were occurring, 2) that the directors did not make a good faith effort to prevent or remedy the situation, and 3) that such failure proximately caused damage to the company.

In the context of cybersecurity breaches, shareholders may claim that, in the case of very large breaches, senior management and directors were either aware or should have been aware of the breach and the company's susceptibility to hacking incidents. If the affected company has experienced previous breaches of cybersecurity, then shareholders may have grounds for arguing that the directors ignored or consciously disregarded prior "red flags" and did not make a good faith effort to remedy the company's vulnerabilities.

Shareholders bringing derivative lawsuits related to cybersecurity breaches face a variety of hurdles. First and foremost, the laws of most states require shareholders to either make a formal demand on the Board or argue that demand is excused because of director interestedness or lack of independence. Potential derivative plaintiffs also face the protective standard of the business judgment rule. These hurdles may prove formidable for derivative suits based on cybersecurity, which involve complex computer systems and require subjective judgments of whether a company is at risk for attacks and whether increased protective measures are necessary. Regardless of whether such shareholder derivative suits are successful, companies should still be prepared to bear the costs of responding to and investigating shareholder demand letters.

Conclusion

Cybersecurity is now a hot-button issue meriting increased attention from corporate boards and management. Issuers must not only take appropriate steps to protect their computer networks and information, but they must also disclose the risks associated with potential cybersecurity breaches and provide timely updates when actual breaches occur. Otherwise, they will face a substantial risk of regulatory scrutiny and shareholder litigation.

---

[1] A market is generally described by economists as efficient when stock prices reflect all publicly available information.
[2] *In re Caremark International Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996).