NU PERSPECTIVE

D&O insurance, cyber liability, and a (big) crack in the board's armor

YAHOO AND HOME DEPOT RECENTLY SETTLED CYBER CLASS ACTIONS. WHAT DOES THAT MEAN FOR YOUR BOARD OF DIRECTORS?

BY JOSHUA GOLD

WHILE THE warning signs of cyber exposures for senior management have been lurking for a few years now, the proverbial proof in the pudding was provided recently when news broke that Yahoo settled shareholder class action litigation with an $80 million payment to the claimants. While this settlement sum alone will never go down as the largest, it is a sizeable departure from past resolutions of cyber securities suits — by a lot. In fact, the trajectory seen with cyber class action consumer claims may have similar (and ominous) parallels for shareholder cyber class actions.

CONSUMER CLASS ACTIONS PORTEND SHAREHOLDER CLASS ACTIONS

Shareholder derivative lawsuits against officers and directors in the wake of data breaches are not a new development. Several have been filed over the last few years against officers and boards accused of permitting lax cybersecurity to inflict financial harm to the corporation and their shareholders. Almost all of these early shareholder suits were dismissed with prejudice, thereby notching early wins for officers and directors against such claims.

But things took a bit of a turn last year when Home Depot settled its shareholder derivative litigation for more than $1 million paid in attorneys' fees to the class action plaintiffs' counsel and agreed to a variety of settlement terms for prospective cybersecurity and oversight measures.

What was particularly interesting about Home Depot's settlement with the class action attorneys is that it came on the heels of multiple (and early) litigation wins by policyholders facing cyber-related shareholder derivative lawsuits. Perhaps even more curious is that Home Depot settled with the underlying class action claimants when the company had already won dismissal of the shareholder class action lawsuit at the trial court level. That decision was on appeal when Home Depot made the decision to resolve the litigation through its settlement.

Was Home Depot's settlement a first crack in the armor? Several months later, Yahoo settled shareholder litigation commenced against it in early 2017, involving the reported hacking of 3 billion Yahoo email accounts. As noted above, a recent report indicates that the Yahoo shareholder litigation settlement amount is sharply higher than any other shareholder litigation settlement involving hacking — $80 million.

If one traces the evolution of consumer class action cyber lawsuits, certain similarities may be discerned with the emerging pattern of cyber shareholder exposures. When company computer security is breached, affecting sensitive individual consumer or patient information, a sure bet is that consumer class action litigation will follow.

As a wave of breaches hit retailers, financial institutions and medical service firms, class actions were brought against them, but mainly lost

(and at an early stage of litigation). However, along the way, a couple early settlements of significant size were made without waiting for a victory on dismissal or summary judgment.

Then, the U.S. Circuit Court of Appeals for the Seventh Circuit weighed in with a pair of reversals in favor of the class action plaintiffs, reinstating class action suits in favor of the consumers against their retailers. At that point, we had a whole new ball game.

The Sixth Circuit followed suit in a subsequent ruling against a financial institution, and some other district courts have since refused to rule against the class action suits brought on behalf of consumers who had their information compromised.

It's likely that we are in the early stages of a similar trend when it comes to shareholder cyber litigation. Early wins for officers and directors may be fleeting, and it may take just one appellate court to change the tide. As such, Home Depot's resolution of shareholder litigation (even after victory at the trial court level), may be seen as a prudent move. Furthermore, no matter what developments occur with shareholder litigation, officers and directors have to be extremely wary of regulator involvement in cybersecurity.

The Securities and Exchange Commission has signaled through words and deeds that it intends to be fully active when it comes to public companies that have been lax in securing their information systems and processes. Indeed, the SEC opened an investigation into Yahoo last year after new revelations emerged about the volume and dates of the compromise.

D&O INSURANCE BECOMES MORE ESSENTIAL

Directors' and officers' insurance becomes more essential when the stakes rise for officer and director liability exposures. So far, D&O insurance has responded to some cyber insurance claims and provided protection — as it should. Even for those companies purchasing dedicated (and standalone) cyber insurance products, directors and officers still will need their D&O insurance protection. Many cyber policies impose an express exclusion for securities claims. Thus, noticing a cyber securities lawsuit for coverage under a cyber policy will surely trigger a coverage fight with many cyber insurance companies.

Further, D&O insurance remains one of the broader liability insurance policies around, offering a strong scope of coverage for an officer's or director's (and sometimes a corporation's) "wrongful acts." Outside of a few select exclusions (like "ERISA," asbestos and nuclear claim exclusions), almost all perils leading to allegations and claims of wrongful acts committed by an insured in their management capacity are covered. Thus, in the ever more perilous cyber environment, it is essential that boards and the executive management team maintain the availability of D&O insurance for cyber-related claims.

SAFEGUARDING YOUR D&O INSURANCE FOR CYBER CLAIMS

With increases in cyber exposures for senior management, D&O insurance underwriters may begin asking questions about cyber hygiene and history, and processes on applications for insurance (whether on new business or renewals). It is critical to make sure that applications for D&O insurance and cyber insurance are answered carefully and accurately. Some insurance applications ask questions that are calculated to be broad, tricky and vague. This can present a terrible trap for policyholders, just when they need their coverage most. Therefore, be smart about how you answer the applications and make sure you have the requisite information to do so.

Consider your retroactive coverage date and push for better terms whenever possible. Many insurance companies want to provide insurance protection only from the date that the first policy they sold you incepts. The problem is that some cyber threats occur well before the policyholder actually discovers evidence of a breach. Further, class action complaints may make vague allegations of a longstanding corporate environment of lax cybersecurity that may stretch back years before the lawsuit's commencement (as well as long before the date of the cyber incident).

Computer forensic specialists will tell you that computer hackers can intrude into computer systems weeks, months and even years before the policyholder becomes aware of the threat. If you purchase insurance coverage with a retroactive date that pre-dates the policy period, especially by a number of years, it removes a potential coverage fight from the table.

Provide notice to your insurance companies quickly after a breach — including your D&O insurance companies. Early in the process of responding to a breach, the meter will be running on costs, and some of those costs may be to protect, investigate and defend the board.

It's important to make sure that D&O insurance coverage (including primary, excess and Side A, for example) remains free of cyber-related exclusions or sub-limits. Management will be highly concerned with any argued "gap" in coverage should a cyber event ensue — especially with the advent of cyber derivative shareholder litigation.

Joshua Gold is a shareholder in Anderson Kill's New York office. He can be reached at jgold@andersonkill.com. This article was first published on Anderson Kill's website and is republished here with permission