Class action puts bulls eye on Target's directors and officers

ALERT | FEB 25, 2014

As if the executives at Target did not have enough to worry about, Target shareholders recently filed a shareholder derivative lawsuit against 14 of Target's directors and officers. The complaint is the second shareholder derivative suit filed against these officers and directors.

Plaintiffs allege four counts against the directors and officers: Breach of Fiduciary Duty; Gross Mismanagement; Waste of Corporate Assets; and Abuse of Control.

In the Complaint, Plaintiffs allege that the directors and officers breached their duties of loyalty and good faith by allowing Target to release false and misleading statements, by failing to properly oversee Target's business and operations, and by failing to prevent certain directors and officers from taking such illegal actions. Plaintiffs further allege that the directors and officers are directly responsible for authorizing or permitting the authorization of, or failing to monitor, the practices which resulted in the "worst data breach" in American retail history and the dissemination of false and misleading statements regarding the scope of that breach. The action alleges that each of the directors and officers had knowledge of, actively participated in, and approved of the wrongdoings alleged or abdicated his or her responsibilities with respect to these wrongdoings.

Plaintiffs also allege that Target was on notice, prior to the breach, that its point of sale system was vulnerable and deficient. Specifically, Plaintiffs highlight a publication authored on Aug. 27, 2007 by Dr. Neal Krawetz that was titled "Point-of-Sale vulnerabilities." Notwithstanding the warnings, it is alleged that Target failed to take appropriate action in response.

The shareholders state that once the data breach occurred, Target made numerous mistakes. First, Target failed to take the necessary steps to notify Target's customers of the data breach. Target's customers had to find out through third parties that their information had been compromised. Plaintiffs allege that this late or improper notification was exacerbated by the fact that once Target acknowledged it had experienced a data breach, it was not forthright with the true depth of the breach. On Dec. 19, 2013, the CEO released a statement indicating that 40 million credit and debit card accounts were compromised. The next day the CEO stated that the problem had been identified and eliminated. To ease the tension, Target offered any Target customer a 10 percent discount on Dec. 21 and 22, 2013.

The Complaint goes on to allege that to avoid a drop off in holiday sales, the directors and officers made the decision to minimize reports regarding the extent of the data breach. This decision appears to have only further eroded customers' confidence when the truth was finally revealed, allegedly causing greater damage to Target's reputation, brand and goodwill.

Within days, third parties reported that the breach was far greater than what was suggested by Target. On Dec. 23, 2013, Target acknowledged that the U.S. Secret Service and the Department of Justice (DOJ) were investigating the matter. Attorneys General from Massachusetts, New York, Connecticut, South Dakota, Illinois, California, Minnesota, and others also notified Target that they were conducting an investigation. The following day, news broke that encrypted PIN data had also been compromised during the breach and that those codes could allow the thieves to access affected customers' bank accounts. Target denied that allegation.

On Dec. 27, 2013, Target admitted that customers' PIN data had been compromised. On Jan. 10, 2014, Target admitted that 70 million more customers' personal information may have been affected, bringing the total count of possible victims up to 110 million Target customers – more than one-third of all Americans.

Plaintiffs allege that, as a result of the foregoing facts, Cowen & Co. dropped Target's expected share price on Jan. 21, 2014 from $66 per share down to $47 per share. Target shares were above $63.50 on Dec. 18, 2013 and since, the data breach shares have fallen over 10.5 percent to $57.60. Target announced on January 22, 2014 that it was cutting health coverage for part-time workers in addition to laying-off 475 workers and eliminating 700 open positions. Plaintiffs allege that this was a result of the data breach. Plaintiffs also highlight the following as alleged damages to Target:

- Costs incurred from the Company's internal investigation into the data breach, including, but not limited to, expense for legal, investigative and consulting fees;
- Costs of updating customers regarding the status of the breach;
- Costs incurred providing credit monitoring for 110 million affected customers;
- Costs incurred defending and settling the numerous class action lawsuits being brought against the Company for the breach;
- Costs incurred from notifying customers, replacing cards, sorting improper charges from legitimate charges, and reimbursing customers for fraudulent transactions (early estimates put this at roughly $5.10 per card, or $561 million);
- Costs incurred from the Secret Service, DOJ and U.S. Senate investigations into the data breach, including, but not limited to, liability for any potential fines; costs incurred from notifying customers and rectifying secondary breach caused by imitation credit monitoring emails; loss of revenue and profit resulting from Target's offer of a 10 percent discount to U.S. shoppers during the last weekend before Christmas in an effort to lure customers back into its stores; costs incurred from instituting chip-based credit cards that will enhance security; and
- Costs incurred from compensation and benefits paid to the defendants who have breached their duties to Target.

WHAT DOES THIS MEAN FOR DIRECTORS AND OFFICERS?

Directors and officers must understand that data breach lawsuits are no longer confined to allegations against the company. In the past, regulatory agencies, state attorneys general,

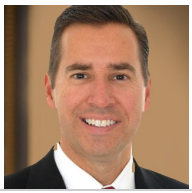
and individuals would focus their efforts on the company to remedy their grievances for compromised information. However, directors and officers are squarely in the crosshairs.

Based upon the dipping stock price and damage to Target's reputation, brand and goodwill, it is no surprise that individuals are now also focusing their efforts on directors and officers. In these lawsuits, the focus has shifted from injury to the individual, to losses incurred by investors, who have allegedly suffered damages due to alleged improper decision-making related to data privacy and security by the directors and officers. Consequently, directors and officers must be better equipped, proactively, to handle data breaches or they might find themselves defendants in a lawsuit.

TAKEAWAY

Cybersecurity is a C Suite issue. Like death and taxes, this too is certain: Directors and officers will see an increase in shareholder derivative lawsuits naming them as defendants for failure to appropriately deal with cybersecurity issues. It is imperative for directors and officers to be proactive and quickly develop an appropriate response. That is the best way to minimize the risk of being named as a defendant. We counsel clients every day about data breach and security issues.

For more information, please contact one of the attorneys listed below.



JAMES GISZCZAK

Read More

DOMINIC PALUZZI

Read More

ADAM SMITH

Read More