Target Data Breach Derivative Suit Dismissed

July 19, 2016 Ronald Breaux, Tim Newman

PRACTICES Privacy and Cybersecurity, Litigation

In a recent ruling, a federal district court in the District of Minnesota dismissed a derivative suit against Target Corporation's board of directors related to the payment card breach Target suffered in late 2013. The dismissal further highlights the difficulty plaintiffs face in sustaining claims arising out of data breaches.

In late 2013, Target suffered one of the largest payment card breaches in history. The breach occurred when malware exposed the card information of 40 million customers and the personal information of 70 million customers. More than 100 lawsuits were filed in the wake of the breach, including a handful of derivative suits that were consolidated in federal court in the District of Minnesota, Target's home state. After suit was filed, a shareholder also made a demand that the board investigate and bring actions against Target's directors and the company's CEO, CFO and CIO.

The derivative suits and related demand alleged that Target's officers and directors (1) failed to properly provide for and oversee an information security program and (2) failed to give customers prompt and accurate information in disclosing the breach. The shareholders brought claims for breach of the fiduciary duties of loyalty and care, corporate waste, gross mismanagement, and abuse of control and identified a variety of damages, including the company's exposure to millions of dollars of potential liability as a result of the breach, the cost of remedial measures (such as the provision of free credit monitoring services to customers whose data had been exposed), a decrease in the company's sales, and reputational damage.

In June 2014, Target established a special litigation committee ("**SLC**") under Minnesota law. Target charged the SLC with investigating the shareholders' allegations, determining whether the company should pursue the shareholders' claims, and responding to the litigation on behalf of the company and its directors. The SLC investigated for 21 months, reviewing thousands of documents and conducting more than 70 interviews.

In March 2016, the SLC submitted a 91-page report concluding that it would not be in Target's best interest to pursue claims against the officers or directors identified in the derivative complaints and related demand. The SLC also determined that it should seek dismissal of the claims and did so in a motion filed in May 2016. In its motion, the SLC outlined relevant Minnesota law that requires a court to defer to the SLC's decision recommending dismissal so long as (1) the members of the SLC possessed a disinterested independence and (2) the SLC's investigative procedures and methodologies were adequate, appropriate, and pursued in good faith.

The plaintiffs stipulated to the dismissal of all shareholder claims in June 2016. In the stipulation, plaintiffs' counsel reserved the right to seek fees, asserting that the plaintiff shareholders' efforts before and during the course of the SLC's investigation were a material factor in creating substantial benefits for Target. Target reserved the right to oppose fees. In a two-page opinion on July 7, 2016, Judge Paul Magnuson of the District of Minnesota granted the SLC's motion to dismiss without analysis. If no shareholder seeks to intervene within 30 days of the court's order,

© 2026 Haynes Boone

the case will be dismissed without prejudice. Plaintiffs' counsel has 30 days from the date of the order to move for fees.

While the outcome of this case is not surprising, it is important for data breach litigators. Many states, including Delaware where many companies are incorporated, permit companies to appoint special litigation committees to evaluate shareholder demands and make recommendations regarding pursuit of those claims. The court's ruling here highlights a hurdle that plaintiffs in data breach litigation may face in seeking to pursue fiduciary duty claims against directors and officers of companies that are the victims of data breaches.

For more information contact one of the lawyers listed below.

© 2026 Haynes Boone