NACD® Directorship
Boardroom Intelligence

Reprinted from NACDonline.org

New Target Ruling Places Your Company's Cyber Oversight in the Crosshairs

By Craig A. Newman and Scott Caplan

Craig A. Newman is a partner at Patterson Belknap Webb & Tyler LLP and chair of its Privacy and Data Security Practice Group. Scott Caplan is an associate in the Privacy and Data Security Practice Group at Patterson Belknap Webb & Tyler LLP.

A recent discovery ruling in the Target Corp. data breach litigation has raised the stakes for corporations and their officers and directors when faced with a cyberattack. The ruling, issued on May 27, 2015 by Magistrate Jeffrey J. Keyes, requires Target to disclose details of similar breaches between 2005 and 2010, including the time frame for the attack, the methods used to access information, measures the company considered and instituted to prevent future breaches, and the extent of the financial fallout.

The Target breach grabbed headlines following the 2013 holiday season as news leaked that hackers had installed malware in Target's security and payments system and captured the credit card information of approximately 70 million shoppers. All too predictably, a series of lawsuits followed that have been consolidated before a federal judge in Minnesota.

This discovery ruling—the most recent development in the Target data breach cases—opens the door to greater scrutiny of corporate cybersecurity decisions and focuses on how past breaches were handled by both senior management, and importantly, by corporate boards.

While the ruling technically applies only to the cases brought by the financial institution plaintiffs in the Target case—banks that had issued the now-compromised credit cards—plaintiffs can be expected to seize upon this ruling and use it as a tactic to argue for similar discovery in other data breach cases. Of particular note are the consequences in class actions and in shareholder derivative suits, where the conduct of corporate leaders is front and center. The ruling opens the door to tough questions about corporate behavior: how were past breaches handled? Were the breaches adequately remediated? Were reasonable internal controls put in place to manage future cyber risks? And, perhaps most importantly, were "red flags" or early warnings of the breach ignored?

Cyberattacks are only becoming more brazen and more prevalent, and data breach litigation is on the rise. Plaintiffs in these suits will use the most recent Target ruling to argue that a company's actions need to be evaluated not only with respect to the existing breach but also with respect to past, or even merely attempted, breaches.

The decision also serves as a reminder of what companies should already be doing. Specifically, there are at least three steps companies should take with respect to their cybersecurity, if they have not already done so.

First, companies should have a data incident response plan in place before a breach occurs. A company's plan should take into account what kinds of data need to be protected, who is likely to try to steal or acquire that data, and who the relevant stakeholders are in the event the data is lost or stolen. Companies should also have their outside counsel and data forensics teams selected and on speed dial.

Second, companies should evaluate their insurance needs for cybersecurity issues. A standard commercial general liability (CGL) policy may ultimately cover some data breach claims, but it could require time and money to establish that coverage, a lesson Sony learned the hard way after North Korean hackers infiltrated its systems. Sony lost its coverage dispute with its CGL carrier at the

trial court and settled the dispute before the appeal was heard. A specialized cyber policy can help avoid a situation like Sony's. In addition, public companies should consider what disclosures they make to investors about cybersecurity risks in light of their insurance coverage.

Third, knowing that plaintiffs in other data breach cases will likely seek discovery of prior breach incidents, companies must adopt and document clear policies that outline the steps being taken to protect sensitive data, along with their responsibilities and plans for disclosing breaches. They should clearly define the roles of senior management and directors and specify the frequency with which security policies are updated.

Cyberattacks are not going away. Companies that proactively adopt sound cybersecurity policies and practices will find it far easier to defend themselves when their businesses come under attack.