Published on *The National Law Review* https://natlawreview.com

# Appeal in Home Depot Data Breach Derivative Action Results in Settlement of Corporate Governance Claims

Article By:

Kevin M. McGinty

Snatching victory of a sort from the jaws of defeat, shareholders who brought a derivative action alleging that the 2014 Home Depot data breach resulted from officers' and directors' breaches of fiduciary duties have reached a settlement of those claims. As previously reported, that derivative action was dismissed on November 30, 2016. That dismissal followed on the heels of dismissals of derivative actions alleging management breaches of fiduciary duties in connection with the Wyndham and Target data breaches. Despite that discouraging precedent, the Home Depot shareholder plaintiffs noticed an appeal from the trial court's order of dismissal. The parties subsequently resumed settlement discussions that had broken off in the fall of 2016, on the eve of argument and decision of Home Depot's motion to dismiss. On April 28, 2017, the parties submitted a joint motion disclosing and seeking preliminary approval of the proposed settlement. If approved, the proposed settlement would result in dismissal of the shareholders' appeal and an exchange of mutual releases, thereby terminating the fiduciary claims arising from the Home Depot data breach.

The Stipulation of Settlement filed with the court specifies that Home Depot will agree to implement the following nine changes to its information governance practices (which are a checklist of best practices for any business):

1. Document the duties and responsibilities of the Chief Information Security Officer ("CISO");

2. Periodically conduct Table Top "Cyber Exercises" to prepare for emergencies and train personnel to respond to data security threats;

3. Monitor and periodically assess key indicators of compromise on computer network endpoints;

4. Maintain and periodically assess the Company's partnership with a dark web mining service to search for confidential Home Depot information;

5. Maintain an executive-level committee focused on the Company's data security;

6. Receive periodic reports from management regarding the amount of the Company's IT budget and what percentage of the IT budget is spent on cybersecurity measures;

7. Maintain an Incident Response Team and an Incident Response Plan;

8. Maintain membership in at least one Information Sharing and Analysis Center (ISAC) or Information Sharing and Analysis Organization (ISAO); and

9. Retain their own IT, data and security experts and consultants as they deem necessary.

It is unknown whether Home Depot had independently contemplated implementing any of these practices in the aftermath of the breach.

The proposed settlement assigns credit for the changes to the derivative action and, by making them part of a court-approved settlement, does allow for judicial enforcement in the event that Home Depot fails to comply with the remediation program. More significantly, wrapping these practices into the derivative action settlement provides a justification for the shareholders' counsel to request a fee award of $1,125,000. Significantly, Home Depot continues to deny any wrongdoing, and the Settlement Agreement expressly states that it may not be construed as evidence or admission of fault, liability or wrongdoing.

The amount of the requested fee award, which is relatively modest by the standards of large scale derivative litigation, suggests that this may have been a nuisance value settlement of an appeal with slim prospects for success. Given the prior failures of derivative claims in data breach cases, it remains to be seen whether this settlement will encourage shareholders in future data breach cases to attempt to buck the odds by asserting derivative claims.



National Law Review, Volume VII, Number 122