Bloomberg BNA

Corporate Law & Accountability Report™

DERIVATIVE SUITS

A Firewall for the Boardroom: Best Practices to Insulate Directors and Officers From Derivative Lawsuits and Related Regulatory Actions Regarding Data Breaches

BY JOSEPH W. SWANSON AND JOHN E. CLABBY

Shortly after the massive 2013 Target data breach, shareholders filed four derivative lawsuits against the company's directors and some of its officers (13 CARE 624, 3/20/15). The shareholders alleged that the defendants had breached their fiduciary duties in not preventing and detecting the breach, and in failing to adequately disclose and otherwise respond to the breach.

Now, more than 18 months after the breach, the derivative suits have been consolidated, and the Board's Special Litigation Committee continues to investigate the allegations. In a recent filing, the Committee reported that it had met 75 times, reviewed thousands of documents, and conducted approximately 60 interviews, with more work to come, including consultation with experts regarding corporate governance and cybersecurity.

Joseph W. Swanson and John E. Clabby are of counsel in Carlton Fields Jorden Burt's Tampa office, where they represent companies, executives and directors in investigating data loss events and in securities and corporate governance litigation, as well as in white collar criminal matters. Both are former criminal Assistant U.S. Attorneys and Computer Hacking and Intellectual Property ("CHIP") prosecutors. Swanson can be reached at jswanson@cfjblaw.com. Clabby can be reached at jclabby@cfjblaw.com.

This unpleasant experience for Target's directors and officers will likely become increasingly common. Complex derivative litigation is expensive, fatigues management and has an uncertain outcome. Worse still, the specter of an Securities and Exchange Commission or other regulatory enforcement action can further complicate a company's post-breach investigative efforts.

This article provides corporate counsel with the practical tools to prepare their directors and officers for a data breach, with an eye toward both fulfilling the respective fiduciary duties and proving the fulfillment of those duties when later challenged in a derivative lawsuit or regulatory enforcement action. Directors and officers who follow and document the steps outlined below will become harder targets for derivative plaintiffs and regulators seeking fees, fines and boardroom trophies.

Cyber 'Caremark': Fiduciary Duties For Data Protection

Board and officer fiduciary duties arise under state law. The fiduciary duty of care is process-focused and requires directors to invest sufficient time, skill and effort into their work such that their decisions aim to advance the company's best interests. The fiduciary duty of loyalty and the related duty of good faith together require directors to place the company's interests ahead of theirs and avoid self-dealing. Officers are held to the same standards as directors. Both constituencies enjoy the protection of the business judgment rule, where courts will not second-guess business decisions if there are no particularized allegations of a fiduciary breach.

In the data breach context, one derivative claim likely to gain prominence is the so-called *Caremark* claim, which is premised on a lack of oversight. Under Delaware law, this claim (named after the seminal case that

 ISSN 2330-6300

outlined its contours) falls within the duties of loyalty and good faith. This is significant because, while companies may insulate their directors from monetary damages for breaches of the duty of care, they may not do so for breaches of the duties of loyalty and good faith.

The standard for a *Caremark* claim is high—a plaintiff must show either that the defendants ''utterly failed'' to implement a reporting system or controls, or that the defendants consciously failed to monitor or oversee the operations of such a system. That exacting standard, however, has not prevented plaintiffs from alleging these claims in derivative litigation, including in the Target case.

In a derivative lawsuit, a shareholder seeks to remedy an injury suffered by the corporation. A shareholder typically first sends a letter to the Board demanding that the company sue the directors and officers who allegedly caused the harm.

Faced with such a demand, a Board has options that include forming a Special Litigation Committee to investigate and determine if a lawsuit is in the corporation's best interests. Most states allow the corporation 90 days to respond to the demand, after which the shareholder may sue on behalf of the company and assert that the refusal of the demand was wrongful. In the ensuing litigation, the defendants will generally point to the Board's or Special Litigation Committee's decision, if any, to reject the demand and will argue that this decision is subject to the business judgment rule. But, as the Target defendants know all too well, Committee work and any trailing litigation are expensive and fraught with uncertainty.

The Coming Wave: Derivative Litigation in the Wake of Data Breaches We believe that derivative litigation will proliferate in the wake of data breaches at public companies. To be sure, consumer class actions alleging negligent failure to safeguard data have gained most of the press and will persist. In fact, corporate counsel at U.S. companies expect increased numbers of class actions alleging data privacy failures.[1] But the plaintiffs' bar has enjoyed mixed success in those cases, with standing, causation and other issues posing hurdles to recovery or at least laying sufficient uncertainty to caution a plaintiff firm's investment.

Conversely, many hurdles that constrain consumer class actions are absent in derivative litigation. First, in derivative suits there is no problem of alleging and ultimately proving class-wide loss, because a single shareholder can bring a derivative action founded on an alleged harm to the company, such as the expense of containment (legal fees, notifying affected consumers), damage in the form of regulatory actions, and loss of customers scared off by the breach.

Second, the initial investment for a derivative suit is minimal for a plaintiffs' lawyer, who need only find a shareholder client and write a demand letter. In many instances, that letter parrots a company's press release regarding a breach, a regulator's announcement of an investigation, or the language in a class action complaint already on file.

Third, given the expense of investigating and responding to a demand, coupled with the cost of defending litigation on the merits, a corporate counsel's simple calculus as to a derivative suit may lead to an early settlement with little work expended by the shareholder's attorney.

Finally, most states' laws provide for the shareholder's firm to recover its fees upon a successful resolution of the derivative action, whether through settlement or at trial.

These factors point to derivative litigation as the future of data breach litigation. Indeed, in addition to the derivative litigation filed after the Target data breach, a similar suit was filed after the data breaches at Wyndham Worldwide Corp. (12 CARE 1360, 10/24/14), and a Home Depot shareholder recently filed an action seeking access to records that likely foreshadows a derivative action related to that company's high-profile data breach last year (13 CARE 1352, 6/19/15).

In the cyber context, shareholders will assert that management and the Board failed to supervise and invest in the company's risk management and data security functions and ignored red flags, all of which contributed to the breach. Shareholders will likely also contend that the defendants failed to respond to the breach in a timely, complete and forceful manner, thereby exposing the company to further harm.

Double Trouble: Enforcement Actions by Regulators Accompanying the likely rise of shareholder derivative actions—indeed, facilitating that forecasted increase—is a heightened focus by state and federal regulators on data breaches.

For example, earlier this year the SEC announced the results of a cybersecurity examination sweep for dozens of registered broker-dealers and investment advisers, and the agency stated that this topic would feature prominently in future examinations. And there have been multiple reports of ongoing enforcement investigations involving data breaches.

While the SEC continues to grapple with asserting a basis for any enforcement activity of public companies—whether grounded in disclosure obligations, internal controls requirements, or some combination thereof—the agency's desire to become a major player in this arena is unmistakable.

The SEC has often stated its interest in policing disclosures around cybersecurity and data breaches for public companies, a focus that would impact the boardroom directly for a wider variety of companies (13 CARE 448, 2/27/15). As early as 2011, the agency released guidance on public companies' disclosure obligations related to cybersecurity risks and data breaches (10 CARE 182, 3/2/12). More recently, in opening remarks at the SEC's Roundtable on Cybersecurity in March 2014, Chair Mary Jo White cited that guidance and noted that the agency's jurisdiction over cybersecu-

[1] See *The 2015 Carlton Fields Jorden Burt Class Action Survey*, available at http://ClassActionSurvey.com/.

   ISSN 2330-6300

rity included the ''disclosure of material information'' (12 CARE 370, 4/4/14). Given the SEC's focus on this topic, many believe that updated directives, perhaps in the form of rules on disclosures, are forthcoming.

While the SEC continues to grapple with asserting a basis for any enforcement activity of public companies—whether grounded in disclosure obligations, internal controls requirements, or some combination thereof—the agency's desire to become a major player in this arena is unmistakable. As SEC Commissioner Luis Aguilar warned in a 2014 speech, ''[B]oards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril'' (12 CARE 648, 6/13/14).

How to Win: The 'Palkon' Blueprint for Success Increased scrutiny by regulators, combined with the likely spike in derivative litigation, means that directors and officers must make cybersecurity an enterprise-level priority.

The good news is that the same corporate governance practices that should insulate directors and officers from derivative liability should also protect those companies from exposure to regulators. Corporate counsel should focus on process over perfection. While data breaches are inevitable for most companies, courts and regulators will look favorably on directors and officers who ensured their companies had in place *processes* to assess risk, deploy resources appropriately, detect breaches, and respond to any incidents in a meaningful, timely way.

Directors and officers must make data breach prevention and detection part of their enterprise risk management, in which breaches are treated like other major risks to the company.

In that regard, directors and officers—and the counsel who advise them—would be well served to review the opinion dismissing the derivative suit filed against Wyndham Worldwide Corp.'s directors and officers. See *Palkon v. Holmes*, No. 2:14-CV-01234 (SRC), 2014 BL 293380 (D.N.J. Oct. 20, 2014) (12 CARE 1360, 10/24/14). In that suit, the plaintiff asserted that the hospitality company suffered injury as a result of three data breaches it experienced, and that the damage was the result of the defendants' failure to adequately oversee the company's cybersecurity. The plaintiff pursued a *Caremark* theory of liability, alleging that the defendants (i) failed to implement security measures to prevent hackers from acquiring customer information, and (ii) did not timely disclose the breaches.

After Wyndham's Board rejected the plaintiff's demand, the plaintiff sued. In October 2014, the district court dismissed that suit with prejudice. While the opinion focused on the propriety of the refusal of the demand, the court's inquiry touched on the measures employed by the defendants to address the data breaches. The court noted with approval that the Board discussed the cyberattacks at 14 meetings over a nearly four-year period. At those meetings, the general counsel gave presentations on the breaches and the company's overall data security. Also, the Audit Committee discussed the same issues at 16 meetings over that period. Further, the company retained technology firms to investigate the breaches and make recommendations on strengthening Wyndham's cybersecurity that the company then began to implement.

The engagement of directors and management in cybersecurity—even where that focus could not prevent multiple breaches from occurring—can reduce, if not eliminate, liability.

Putting Up the Firewall: Preparing for and Responding to the Breach Directors and officers must make data breach prevention and detection part of their enterprise risk management, in which breaches are treated like other major risks to the company. Corporate counsel should ensure that their companies implement the following action items, involving the Board and senior management as specified:

1. Assess the risk by identifying (i) the types of data held by the company, (ii) the likelihood of each bucket of data being accessed or acquired by an outsider, and (iii) the impact on the company if such access or acquisition occurred.

2. Draft policies and procedures for the handling of data, and then test and audit them.

3. Draft an incident response plan that is tailored to the company's regulatory and legal environment and business risks and that outlines what steps to take if its data were compromised, including whom to call for help and how to notify consumers. Include any thresholds for Board reporting, calibrated to the level of breach. As with internal audit findings, minor data-breach incidents may be aggregated and reported periodically to the appropriate committee. Major incidents require immediate reporting to the Board.

4. Provide periodic training to relevant staff both on the company's incident response plan and its policies and procedures.

5. Review the company's existing insurance policies and consider obtaining cyber-insurance to address any exposure.

6. Create a Board committee or task an existing Board committee such as the Audit Committee or Technology Committee to focus on data protection issues (''Cyber Committee'') and adjust the committee charter as necessary. Designate a lead Board member for data privacy issues (''Lead Cyber Director'') to foster greater informal contact with the Board on key issues and in crises.

7. Create a Chief Information Security Officer (CISO) or equivalent position with reporting duties to the CEO or directly to the Cyber Committee. In either event, allow and encourage direct, unfiltered contact between the Board and the CISO.

8. Periodically retain a consulting firm to review and test the company's policies and procedures, information technology and physical security, and overall preparedness for a data breach. The firm can generate a report of its findings, which should

be shared with the Board or Cyber Committee in written, summary form.

9. Brief the Cyber Committee at least quarterly on major changes to items 1-5. Brief the entire Board on items 1-5 at least annually. Involve outside counsel and consultants in direct briefings to the Board if the company's risk is especially sensitive or there has been a major regulatory change.

10. Memorialize all of the foregoing efforts. Meeting minutes should reflect the questions related to cybersecurity and the deliberation given to those issues. If outside consultants give presentations, memorialize those in the minutes. Corporate counsel should track Board and Cyber Committee activity related to cybersecurity for later, prompt use in litigation or regulatory investigations.

While these measures help minimize risk, they are hardly failsafe. In the event of a data breach, the directors and officers should bear in mind the following to contain the damage and limit liability:

1. The business units and IT staff should activate the incident response plan, which will include assessing whether the incident warrants Board notification. Borderline incidents should be discussed with the Lead Cyber Director.

2. For major incidents, the officer who reports to the Board on cybersecurity issues in the ordinary course (preferably the CISO) should immediately arrange a telephonic Board or Cyber Committee meeting to report the breach.

3. During the briefing, management must provide the directors with key information as to cause, scope, containment and outside notification, even if some information remains unconfirmed. What is important is briefing the Board early and often. If management has retained outside investigators and counsel, give the Board access to those firms for unfiltered dialogue.

4. Keep accurate minutes that reflect the level of information shared with the Board and the directors' discussion of the issues.

5. After the breach has been contained, evaluate the response and revise the incident response plan and policies and procedures to be ready for the next time. Present the findings and remediation plan to the Board.

Wrapping Up: Process Trumps Perfection

A breach by itself is not likely to be the basis for liability. Rather, shareholders, courts and regulators will look at what the company's directors and officers did before and after the incident to protect the corporate interests. In the end, a documented process will be key for directors and officers to avoid liability.

   ISSN 2330-6300