BRACEWELL

INSIGHTS

Lessons For Corporate Directors From The Wyndham Data Breach Derivative Action

December 18, 2014

By: ***David J. Ball***

To listen to the podcast, ***please click here***.

On October 20, 2014, Wyndham Worldwide Corporation won dismissal of a shareholder derivative suit seeking damages arising out of three data breaches that occurred between 2008 and 2010. *Dennis Palkon, et al. v. Stephen P. Holmes, et al.*, Case No. 2:14-cv-01234 (D. N.J. Oct. 20, 2014). Wyndham prevailed, but the litigation carries key lessons for directors seeking to avoid oversight liability in connection with cybersecurity breaches.

Businesses suffering data breaches end up litigating on multiple fronts. Wyndham had to defend itself against the shareholder derivative action and against a Federal Trade Commission action. Companies also likely will face section 220 books and records demands as a precursor to derivative claims. Also, in other data breach-related cases, the Securities & Exchange Commission, the Department of Justice, and state regulatory agencies have asserted jurisdiction. Regulatory actions only compound exposure from private civil actions.

The Wyndham litigation underscores that directors must proactively examine their cybersecurity policies and systems. Savvy corporate directors deliberate their cybersecurity defenses, confer with knowledgeable professionals, and implement corporate procedures and controls that not only bolster those defenses and identify red flags, but also include crisis response plans in the event those defenses ultimately are breached. Additional measures directors should consider to protect against cyber-attacks (and resulting oversight claims) include periodically stress-testing the company's defenses, hiring a Chief Information Security Officer and routinely disposing of records that the company no longer needs for business purposes, but which include personal information.

Case Summary

Between April 2008 and January 2010, hackers breached Wyndham's network on three occasions and obtained the personal and financial data of over 600,000 customers. The FTC investigated and in June 2012, commenced legal action against Wyndham. *Federal Trade Commission v. Wyndham Worldwide Corp., et al.*, Case No. 2:13-cv-01887 (D. N.J.). Years later, a Wyndham shareholder demanded that its board bring a lawsuit against the company's officers based on the data breaches. The board's audit committee declined to pursue the suit, a decision that the board adopted. *Palkon*, at 2-3.

In February 2014, the shareholder filed a derivative lawsuit against Wyndham, its officers, and its directors, claiming that the company's failure to implement adequate cybersecurity

measures and disclose the data breaches in a timely manner caused the company to suffer the damages of an FTC investigation. The lawsuit also claimed that the board wrongfully decided not to pursue litigation. Wyndham moved to dismiss, asserting that the board's decision was a valid exercise of its business judgment. *Id.* at 4.

The Court's Analysis

A board's decision to refuse a shareholder's demand to commence a litigation is afforded a rebuttable presumption that the refusal was a proper exercise of its business judgment so long as the decision was made "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company." *Id.* at 5 (citing *Spiegel v. Buntrock*, 571 A.2d 767, 773 (Del. 1990)). To rebut that presumption, the plaintiff must plead with particularity facts that give rise to a reasonable doubt that the board either acted in good faith or conducted a reasonable investigation. The Court held that Plaintiff failed to meet this burden for the following reasons:

- Plaintiff's allegations that Wyndham's counsel suffered from a conflict because it represented Wyndham in the FTC action and in connection with the shareholder demand failed to give rise to a reasonable doubt regarding whether the board acted in good faith. The Court reasoned that Wyndham's counsel's "obligations in the FTC and shareholder matters were identical: it had to act in [Wyndham's] best interest." Likewise, the Plaintiff's allegations regarding alleged conflicts of interest on the part of Wyndham's General Counsel were too conclusory to establish an inference of bad faith.

- Plaintiff's allegations were insufficient to raise an inference of gross negligence in order to create a reasonable doubt regarding the reasonableness of the board's investigation because the board took numerous steps to familiarize itself with the demand, already had substantial familiarity with the cyber-attacks in connection with the FTC action and previously had discussed the cyber-attacks at numerous board and committee meetings.

The Court also noted that the board was free to consider the merits of the proposed lawsuit when it rejected the shareholder's demand. In this regard, even though it did not need to reach the merits of Plaintiff's claims, the Court characterized the claims as "novel," emphasizing Plaintiff's concession that security measures existed at the time of the first breach and that the board addressed the attendant risks numerous times.

Lessons Learned

The *Wyndham* litigation provides several important lessons for businesses that may be subject to a data breach:

- Prior to suffering a data breach, businesses should confer with knowledgeable counsel and technology consultants to implement cybersecurity measures and compliance procedures. Such procedures should include identifying cybersecurity red flags, periodically stress-testing defensive measures and creating a crisis response plan. Companies should also consider hiring a Chief Information Security Officer and periodically disposing of unnecessary records containing personal information.

- Following a data breach, businesses must be prepared to respond to civil legal proceedings and government regulatory inquiries and investigations. Regulators are not focused only on financial institutions and retail businesses, but rather on any entity that

maintains sensitive information electronically. And derivative plaintiffs will seek to investigate and challenge the board's oversight of the company's cybersecurity defenses. The best protection from such challenges is having a documented deliberative process resulting in formal prevention and crisis response plans that were routinely monitored.

- Management and/or the board of directors may have to defend the company's conduct in parallel actions: a civil suit and a regulatory investigation. Defending its cybersecurity in a civil case while simultaneously identifying its cybersecurity flaws in a regulatory action places businesses in a tenuous, uncomfortable position, and is all the more reason to act diligently, prudently, and proactively before a breach occurs.