BRACEWELL

INSIGHTS

Consequences of a Data Breach: Lessons from Wyndham Worldwide

October 24, 2014

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

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 cybersecurity warnings for officers and directors.

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. 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.

Officers and directors play a key role in cybersecurity. Wyndham's directors supported the company as it defended its conduct and procedures before the FTC. However, they also had to satisfy their fiduciary duties to assess whether the breaches were the result of negligent or reckless conduct by Wyndham's officers, which may have required the company to file its own civil action against its officers. It is not difficult to imagine situations in which a board of directors determines that the company's officers acted wrongfully or negligently and end up with a choice between suing the company's own officers for their conduct or foregoing such a lawsuit and facing derivative litigation from shareholders.

The Wyndham litigation underscores that companies must examine how their cybersecurity policies and procedures may expose them to liability. Companies must take all reasonable measures to implement strong cybersecurity measures and prepare crisis response teams in the event a breach nevertheless occurs.

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 shareholders 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)). In *Wyndham*, the court made the following determinations:

- That Wyndham's counsel, who both represented Wyndham in the FTC action and advised the board not to pursue litigation against the officers, did not have a conflict of interest because counsel's "obligations in the FTC and shareholder matters were identical: it had to act in [Wyndham's] best interest." *Id.* at 6-7.

- That the board had a firm grasp of the litigation demand by the shareholder, had conducted a diligent investigation, and had specifically met to consider the data breach and cybersecurity issues. *Id.* at 9-11.

- That the shareholder's claim that the board breached its fiduciary duty by refusing the litigation demand was "novel" and dubious, and that Wyndham had appropriately responded by employing five advisory firms on cybersecurity issues and implementing post-breach security measures. *Id.*

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. Strong cybersecurity measures weaken any argument that a business or its management is reckless or has otherwise failed to satisfy an appropriate standard of care.

- 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.

- 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.

If you are interested in hearing more about data privacy/cybersecurity please contact any of

the following or the Bracewell attorney with whom you usually work: In Dallas: ***Shamoil Shipchandler*** In New York: ***Dan Meyers*** or ***David Ball*** In Seattle: ***Curt Hineline*** In Washington, D.C.: ***Dee Martin*** or ***Shelby Kelley***