New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 251—NO. 85
MONDAY, MAY 5, 2014

Outside Counsel

Expert Analysis

FTC Can Regulate Data Security, But It's Not a Blank Check

By **F. Paul Greene**

News of data breaches was once relegated to IT-related websites and specialty blogs. It now peppers the headlines of every major news outlet. The recent Target breach has even led to a movie deal.

Against this backdrop, the concerns arising from a data breach can be many: a storm of negative press, huge disruptions in operations as a company reacts to and remediates the breach, as well as the looming threat of breach-related litigation. Added to those concerns is the possibility of Federal Trade Commission scrutiny and action. Yet, the FTC has no specific statutory or regulatory guidelines for data security. Rather, it has based its numerous enforcement actions on a broad reading of Section 5(a) of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. §45.

The FTC's authority under Section 5(a) to regulate and punish victims of a data breach, such as a hotel or retail chain, has never been significantly challenged, until recently in a case before the U.S. District Court for the District of New Jersey, *FTC v. Wyndham Worldwide Corp*. In the Wyndham case, Wyndham moved to dismiss the FTC's complaint for failure to state a claim under Fed. R. Civ. P. 12(b)(6). U.S. District Judge Esther Salas recently decided Wyndham's motion in the FTC's favor, but Salas' decision may be limited to the facts of *Wyndham*.

Wyndham Networks

From April 2008 through January 2010 criminals allegedly hacked into Wyndham's networks, compromising over a half-million payment card numbers in one of the largest data breaches to date. Alongside the avalanche of bad press and other repercussions that followed, Wyndham Worldwide Corp., one of the world's largest hospitality companies, soon found itself in the unenviable position of defending against an enforcement action brought by the FTC under Section 5(a).

Specifically, on June 26, 2012, the FTC filed a complaint against Wyndham and its subsidiaries in the U.S. District Court for the District of Arizona. Historically, the FTC had enforced data security obligations through consent order settlements. The Wyndham case, which was subsequently transferred to the District of New Jersey, garnered much attention because it marked a move by the FTC to enforce data security standards by suing a breached entity in federal court.

In *Wyndham*, the FTC alleged that Wyndham failed to maintain reasonable security measures, which allowed hackers to obtain access to customers' sensitive personal information including payment card account numbers, expiration dates, and security codes. The complaint also alleged that the hotel chain misrepresented the security measures it had taken to protect customers' personal information. The FTC claimed that Wyndham's failure to implement "reasonable and appropriate measures to protect personal information" resulted in fraudulent charges on customers' accounts and more than $10.6 million in fraudulent purchases.

The FTC focused on the hotel chain's alleged failure to implement Internet firewalls and data encryption programs, utilize robust passwords for access to Wyndham-branded data systems, employ reasonable measures to detect and prevent

F. PAUL GREENE *is a partner with Harter Secrest & Emery in Rochester and co-chair of the firm's privacy and data security practice.* DANIEL J. ALTIERI, *an associate in the firm's Buffalo office, assisted in the preparation of this article.*

unauthorized access to its computer networks, and follow proper incident response procedures, among other "security insufficiencies." In the Wyndham action, the FTC sought a permanent injunction to prevent Wyndham from violating the FTC Act in the future, as well as money damages to redress consumer injury. In response, Wyndham maintained that it was the victim of cyber-crime and claimed that there was no evidence that it was to blame for the breaches.

Motion to Dismiss

Early last year, Wyndham and its subsidiaries sought to dismiss the FTC's complaint in large part on the grounds that Section 5(a) of the FTC Act does not give the FTC the broad authority to bring a civil claim concerning a data breach and that, in any event, the FTC had not provided fair notice of what it required under Section 5(a) with regard to data security practices. In this regard, the federal government has tried repeatedly to confer explicit statutory authority on the FTC to regulate specific data security standards, but each such attempt has failed to get through Congress. In addition, U.S. Attorney General Eric Holder has recently urged Congress to enact a federal data breach notification standard, in contrast to the patchwork of notification laws existing in 46 states and the District of Columbia.

In its motion, Wyndham went on to argue that Section 5(a)'s general prohibition on unfair and deceptive trade practices was not a specific grant of authority to establish data-security standards for the private sector as a whole. As maintained by Wyndham, an open-ended statutory provision, such as Section 5(a), does not empower an administrative agency to impose sweeping new regulations on businesses in the absence of an explicit authority from Congress.

Wyndham also argued that it could not be accused of deceptive practices because its privacy policy made no representations about the data security at Wyndham-branded hotels (which are, to a large extent, separate entities from Wyndham Worldwide Corp.), Wyndham retained no control over the day-to-day activities at Wyndham-branded hotels, and it therefore could not be held liable for breaches occurring on the networks of Wyndham-branded hotels.

> The FTC's authority under Section 5(a) to regulate and punish victims of a data breach, such as a hotel or retail chain, has never been significantly challenged, until recently in a New Jersey case.

In opposing Wyndham's motion, the FTC argued that Section 5(a) was drafted broadly to allow the FTC to protect consumers from unanticipated threats in a changing economy, such as those posed by modern-day cyber criminals, and that it provided sufficient notice and guidance to businesses through public statements and consent orders involving other companies that failed to protect customer payment card information.

Court's Decision

Wyndham's motion was anticipated to be a watershed moment in the realm of FTC data breach enforcement actions. More than 10 industry participants and subject matter stakeholders submitted amicus curiae briefs, falling on both sides of the issue, but mainly supporting Wyndham's motion to dismiss.

On April 7, 2014, Judge Salas denied Wyndham's motion to dismiss. In doing so, the court rejected Wyndham's "invitation to carve out a data-security exception to the FTC's unfairness authority" and declined to dismiss the FTC's complaint on fair notice grounds, especially in light of the FTC's many public complaints and consent agreements, as well as its public statements and business guidance brochure (not to mention Wyndham's own references to "industry standard practices" and "commercially reasonable efforts" in its privacy policy). The court also determined that the FTC's unfairness and deception claims satisfied federal pleading requirements.

In deciding upon Wyndham's motion, Salas cautioned that the court's decision was limited to the facts of the Wyndham case, and specifically noted that it "does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked." Nonetheless, the Wyndham case, and this recent decision, will have far-reaching ramifications.

As Salas explicitly recognized, albeit with a modicum of understatement, "we live in a digital age that is rapidly evolving—and one in which maintaining privacy is, perhaps, an ongoing struggle." Such an environment gives rise to "a variety of thorny legal issues that Congress and the courts will continue to grapple with for the foreseeable future."

It is as of yet unclear exactly what effects Salas' decision will have, but at least in the short term, companies can continue to count on potential FTC action as one of the many "thorny legal issues" that may arise, when a data breach occurs.

Reprinted with permission from the May 5, 2014 edition of the NEW YORK LAW JOURNAL © 2014 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-05-14-13