Bloomberg BNA

Privacy and Security Law Report®

FTC Enforcement

As we look ahead to 2016, what do the *Wyndham* and *LabMD* rulings mean for the FTC and the organizations under its watchful eye? Although the *Wyndham* settlement sends a symbolically important message—like it or not, the FTC will continue to fill the void left by Congress' failure to adopt wide-ranging legislation on data security—but that message is blurred and potentially undercut by the *LabMD* ruling, the author writes.

The Long and Wyndham Road: A Settlement in *Wyndham* and Curve Ball in *LabMD* Signals Storm Warnings for the FTC's 2016 Data Security Initiatives

By Craig A. Newman

Headline-grabbing data breaches commanded our attention throughout 2015. First, it was Anthem Blue Cross and Blue Shield with nearly 100 million medical records hacked, then the U.S. Office of Personnel Management with more than 20 million records compromised, and finally, Ashley Madison, with the ''affairs'' of 37 million customers exposed for all to see. But despite the seemingly never-ending drumbeat of high profile breaches, it was the Federal Trade Commission (FTC) that stole the show in 2015.

Craig A. Newman is a partner with Patterson Belknap Webb & Tyler LLP and chair of the firm's Privacy and Data Security Practice. He was recently named a 2015 Trailblazer in Cyber Security and Data Privacy by The National Law Journal.

And 2016 Is Likely to Be No Different

Over the past decade, the FTC has reigned supreme over the federal government's private sector data security enforcement. In fact, the Commission has instituted more than 50 data security enforcement actions since 2005 against public and private organizations, almost all of which have resulted in settlements or consent decrees.[1] This despite years of fighting over whether the FTC actually had the authority to bring data security enforcement actions in the first place. Earlier this month came the settlement of the long-running *Wyndham Worldwide Corporation* case, which certainly won't end the debate, but does serve to further reinforce the FTC's role in data security enforcement [2]. Wyndham was one of only two companies to launch a full-scale challenge to the FTC's cyber authority (14 PVLR 2228, 12/14/15).

But now the only other company to do so, LabMD, Inc., has taken center stage in challenging the agency's status as top cop in consumer-related cybersecurity matters. LabMD has been the proverbial thorn the in

[1] Federal Trade Commission, Cases and Proceedings, *available at* https://www.ftc.gov/enforcement/cases-proceedings.

[2] *FTC v. Wyndham Worldwide Corp.*, D.N.J., No. 2:13-cv-01887-ES-JAD, stipulated order filed, 12/9/15, *available at* https://www.ftc.gov/system/files/documents/cases/151211wyndhamstip.pdf.

 ISSN 1538-3423

the FTC's side for years—challenging the Commission's authority, integrity and administrative processes in its long-running data security case. And last month, LabMD delivered a knock-out punch when it convinced the FTC's own Chief Administrative Law Judge to dismiss the Commission's case against the tiny Atlanta-based medical testing lab, finding that the agency failed to demonstrate consumers had suffered a concrete injury as the result of two apparent data breaches—an injury beyond ''mere'' speculation—as required by Section 5 of the FTC Act.[3] (14 PVLR 2109, 11/23/15). The *LabMD* ruling is now on appeal to the full Commission.[4]

As we look ahead to 2016, what does all of this mean for the FTC and the organizations under its watchful eye? While the *Wyndham* settlement sends a symbolically important message—like it or not, the FTC will continue to fill the void left by Congress' failure to adopt wide-ranging legislation on data security—but that message is blurred and potentially undercut by the *LabMD* ruling. It also begs the broader question of whether the FTC may be forced to raise the bar and show a concrete consumer injury as an element of its enforcement actions, just as private plaintiffs have for years as a jurisdictional and substantive matter.

Wyndham: The Settlement

On December 9, 2015, the FTC announced its settlement with Wyndham. The Commission had charged the hotel conglomerate with maintaining poor data security practices that exposed payment information of more than 600,000 consumers in three separate data breaches reaching back to 2008, and racking up more than $10 million in fraudulent charges against credit card customers. Under a stipulated order for injunction filed in the U.S. District Court for the District of New Jersey, key aspects of the settlement include:

- Wyndham must implement and maintain a ''comprehensive information security program'' for 20 years that is reasonably designed to protect the security, confidentiality and integrity of cardholder data that is collected or received by Wyndham-owned hotel and resort properties within the U.S.;
- Each year, Wyndham must secure a written assessment and certification of the hotel group's PCI Data Security Standard (PCI DSS) compliance from an independent, qualified third-party professional. The annual assessment process draws a line between the computer network for Wyndham-owned properties and the networks for licensed properties—called ''untrusted networks.'' Each year, Wyndham must identify the ''untrusted networks,'' and confirm that they remain so, *i.e.*, are not part of Wyndham's network infrastructure. If an ''untrusted network'' becomes ''trusted,'' Wyndham is on the hook for that network and must certify its compliance with the settlement agreement. Wyndham must also undertake a comprehensive risk assessment as laid out in the PCI DSS Risk Assessment Guidelines. If Wyndham obtains this assessment each year, it will not be required to establish the comprehensive information security program noted above;
- In the event of another data breach involving more than 10,000 payment cards, Wyndham would be required to undertake additional forensic work and provide the results to the FTC within a certain time frame;

The settlement—which does not require Wyndham to pay a monetary penalty or admit liability—remains subject to court approval.

Wyndham: The Case

Wyndham's saga with the FTC started in June 2012, when it was sued by the agency in Federal court for ''unfair'' and ''deceptive'' practices under Section 5 of the FTC Act. As a result of Wyndham's lax data security measures, including 3 breaches, the FTC complaint charged, it ''unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft.''[6]

Section 5 of the FTC Act, a 100-year-old statute, generally prohibits ''unfair or deceptive'' acts or trade practices ''in or affecting commerce.'' [7] The FTC has relied on this general grant of authority to pursue enforcement actions for ''unfair'' data security practices. It provides:

''The Commission shall have no authority . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice

[3] *In re LabMD Inc.* (F.T.C. 2015), *available at*https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf

[4] https://www.ftc.gov/system/files/documents/cases/580032_-_labmd_-_complaint_counsels_notice_of_appeal.pdf

[6] *FTC v. Wyndham*, 2015 U.S. App. LEXIS 14839, at *5.

[7] 15 U.S.C. Section 45(a)(1)(2012).

   ISSN 1538-3423

causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.[8]

Wyndham moved to dismiss the case, arguing that the FTC lacked enforcement authority under Section 5 over data security practices. On April 7, 2014, Judge Esther Salas of the District of New Jersey disagreed and refused to dismiss the case, holding that the ''contour of an unfairness claim in the data-security context, like any other, is necessarily 'flexible' such that the FTC can apply Section 5 'to the facts of particular cases arising out of unprecedented situations.' ''[9]

The Third Circuit's *Wyndham* decision answers the threshold question of the FTC's authority to enforce data security standards, at least for now, and at least at the motion to dismiss stage.

The Third Circuit's Ruling

Nearly a year and a half later, a three-judge panel of the U.S. Court of Appeals for the Third Circuit unanimously affirmed Judge Salas's ruling. *Wyndham* is the first federal appellate ruling on the merits of whether data security practices can constitute an ''unfair'' trade practice under Section 5,[10] an issue that has been hotly debated for years.

Wyndham challenged the FTC's jurisdiction to police data security practices on three general grounds. *First*, it argued there was nothing ''unfair'' about Wyndham's conduct. Wyndham was the victim, not the perpetrator, of the hacking, and there was no allegation that Wyndham had acted unscrupulously. Congress's express and specific delegation of cybersecurity enforcement to the FTC in certain targeted statutes, such as the Fair Credit Reporting Act, made little sense if the FTC already had broad authority to regulate in the same domain.[11] *Second*, Wyndham argued that even if the Commission *did* have authority to police cybersecurity, it had not provided fair notice to regulated companies as to what the FTC expected of them. The FTC's publications and consent agreements on cybersecurity, Wyndham argued, consisted of little more than vague generalities and platitudes that were not particularly helpful to regulated entities.[12] *Finally*, Wyndham argued that the FTC's complaint failed to state a claim as a technical matter, because it did not allege a ''substantial injury to consumers'' which was not ''reasonably avoidable by consumers themselves,'' as required by Section 5(n) of the FTC Act.[13]

The Third Circuit rejected each of these arguments. Tracing the history of the FTC's unfairness authority, it held that Congress had defined the Commission's authority broadly and flexibly, intentionally leaving the development of an unfairness standard to the Commission itself.[14] Moreover, the court rejected reading into the statute any requirement that unfair conduct be ''unscrupulous'' or ''unethical.''[15] Equally unavailing was Wyndham's argument that specific cybersecurity statutes evidenced Congressional understanding that the FTC Act had not given the Commission cybersecurity authority. The court read these statutes as supplementing, not contradicting, the FTC's already broad jurisdiction.[16]

The court also held that Wyndham had fair notice that its data security practices could give rise to liability. Taking the FTC's allegations as true on a motion to dismiss—as it must—the court found that Wyndham was on notice that its alleged lack of cybersecurity protections for consumers could constitute an ''unfair'' practice within the meaning of Section 5(a) of the FTC Act.[17] The court's conclusion was ''reinforce[d]'' by the FTC's 2007 guidebook, which ''describes a 'checklist[]' of practices that form a 'sound data security plan.' ''[18] In a similar vein, while the court agreed with Wyndham's argument that the FTC's previous consent orders were ''of little use'' in understanding what Section 5(a) requires, they nonetheless ''help[] companies with similar practices apprehend the possibility that their cybersecurity could fail as well.''[19] The court noted several of

[8] Federal Trade Commission Act Amendments of 1994.

[9] *FTC v. Wyndham Worldwide Corp.*, No. 13-1887 (ES) (D.N.J. Apr. 7, 2014).

[10] *FTC v. Wyndham*, 2015 U.S. App. LEXIS 14839.

[11] Appellant's Opening Brief at 18–35.

[12] *Id.* at 35–45.

[13] *Id.* at 45–50.

[14] *FTC v. Wyndham*, 2015 U.S. App. LEXIS 14839, at *11–*15; *see also FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 240 (1972) (Congress ''explicitly considered, and rejected, the notion that it reduces the ambiguity of the phrase 'unfair methods of competition' . . . by enumerating the particular practices to which it was intended to apply.'')

[15] *FTC v. Wyndham*, at *16 (citing *FTC v. Sperry & Hutchinson Co.*, 405 U.S. 233, 244 n.5 (1972)). *Sperry* was decided when the so-called Cigarette Rule, 29 Fed. Reg. 8355 (1964), was still the operative statement of FTC policy. The Cigarette Rule required the FTC to consider factors, including whether the conduct in question ''is immoral, unethical, oppressive, or unscrupulous.'' Although the unscrupulousness of conduct was a factor to be considered, it was not a necessary condition of an unfair act or practice. *Sperry*, 405 U.S. at 244 n.5. In adopting its 1980 Unfairness Policy Statement, later codified at 15 U.S.C. § 45(n), the Commission observed that it had never relied on the ethics factor ''as an independent basis for a finding of unfairness'' and ''abandoned the theory of immoral or unscrupulous conduct altogether.'' *FTC v. Wyndham*, at *13 (quoting *Int'l Harvester Co.*, 104 F.T.C. 949, 1061 n.43, 1076) (internal punctuation and quotation marks omitted).

[16] *FTC v. Wyndham*, at *22–*28 (distinguishing *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120 (2000)).

[17] *Id.* at 28–47.

[18] *Id.* at *47 (quoting FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* https://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf).

[19] *Id.* at *49 n.22, *50.

the FTC's complaints contained allegations were similar to those against Wyndham.[20]

If LabMD has its way, the FTC will need to deal with "injury" as an element of its enforcement actions in the same way as a private plaintiff, which would raise the bar and the FTC's burden in pursuing future data security enforcement actions.

Finally, the court rejected Wyndham's argument that the FTC failed to allege an adequate consumer injury, noting the FTC's complaint alleged ''unreimbursed fraudulent charges'' and that consumers ''expended time and money resolving fraudulent charges and mitigating subsequent harm.''[21] Without stating so explicitly, the Third Circuit accepted these allegations as sufficient to state a claim under Section 5, at least at the motion to dismiss stage.

LabMD: Act Two

At the same time the *Wyndham* case was being fought out in Federal court, LabMD proceeded on a parallel track as an administrative adjudication.[22] The LabMD saga began in 2010 when the Commission commenced an investigation into the firm's data security safeguards based on two apparent breaches. LabMD, founded 20 years ago, served physicians by analyzing tissue samples for prostate and bladder cancer, and as a result, maintained personal information on approximately 750,000 patients. After several years of contentious back-and-forth, the FTC in 2013 filed an Administrative Complaint alleging that LabMD had failed to adequately protect patient medical data, and demanded that it institute a comprehensive data security program and submit to third-party security audits for the next 20 years. LabMD, however, assumed the role of ''David,'' pushing back and refusing to settle with the regulatory ''Goliath.''

A three-year battle ensued, including a full administrative trial. The docket sheet—with more than 200 entries—more closely resembles a complex antitrust case than a routine administrative proceeding. After wading through the voluminous record, which included more than 1,000 exhibits, 39 witnesses, and 2,000 pages of trial and post-trial briefing, Chief Administrative Law Judge D. Michael Chappell handed the Commission a stinging defeat. In a 91-page ruling, ALJ Chappell dismissed the FTC's case against LabMD on the grounds that the Commission failed to demonstrate that it was ''likely'' consumers had been substantially injured—as required by Section 5—as a result of the two alleged data security incidents dating back nearly seven years.[24]

The *Wyndham* settlement provides a window into the FTC's expectations when other organizations suffer payment card breaches, especially if franchisees or third-party vendors are involved.

ALJ Chappell concluded that the FTC failed to show any proof whatsoever of actual consumer injury. He flatly rejected the FTC's theory that a statistical or hypothetical risk of future harm was enough to find LabMD liable for unfair conduct under Section 5 of the FTC Act. ''To impose liability for unfair conduct under Section 5(a) of the FTC Act, where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical 'risk' of a future data breach and identity theft, would require unacceptable speculation and would vitiate the statutory requirements of 'likely' substantial consumer injury.''[25]

The ALJ did not rule on whether the FTC had jurisdiction to enforce data security standards under the unfairness prong of Section 5, noting: ''Believing the Commission's determination of its jurisdiction to be erroneous, Respondent reserves its jurisdictional challenge for its anticipated appeal to the federal court.''[26]

Implications for the FTC and Cybersecurity in 2016

So, as we approach 2016, what lessons do we take from the *Wyndham* case and its recent settlement, and what might the *LabMD* case foreshadow for the year ahead?

The Third Circuit's *Wyndham* decision answers the threshold question of the FTC's authority to enforce data security standards, at least for now, and at least at the motion to dismiss stage. It also means that the FTC's pronouncements and consent decrees take on added significance for companies evaluating what data security measures will satisfy a Commission inquiry.[27]

[20] *Id.* at 51–54.

[21] *Id.* at *10.

[22] It is within the Commission's discretion to commence either an administrative proceeding or civil lawsuit in Federal court. (https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority). The former process is under scrutiny because the agency wears the dual hat of litigant and adjudicator. And not surprisingly, the Commission has an unprecedented record of success in such in-house adjudications. Indeed, according to one study, FTC counsel had a 20-year winning streak in cases adjudicated before the Commission (on appeal from decisions made by an administrative law judge). *See* David A. Balto, The FTC at a Crossroads: Can It Be Both Prosecutor and Judge? 28 Legal Backgrounder 1, 1 (2013) (http://www.wlf.org/upload/legalstudies/legalbackgrounder/08-23-13Balto_LP.pdf); Joshua D. Wright, Commissioner, Fed. Trade Commission, Remarks at the Global Antitrust Institute Invitational Moot Court Competition, at 17-18 (Feb. 21, 2015).

[24] *In re LabMD Inc.* (F.T.C. 2015).

[25] *Id.*

[26] *Id.*

[27] The FTC's press releases are *available at* https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises. *See also* FTC, *Start with Security: A Guide for Business* (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (describing 10 ''lessons to learn'' from these enforcement actions).

   ISSN 1538-3423

Equally important, the *Wyndham* settlement provides a window into the FTC's expectations when other organizations suffer payment card breaches, especially if franchisees or third-party vendors are involved. Unlike other consent decrees, the *Wyndham* settlement focuses specifically on protecting credit card data as opposed only to general cyber hygiene. It also specifically relies upon PCI DSS as the benchmark, providing some assurance that compliance with this standard or an equivalent will go a long way to providing ''reasonable'' data security and keeping the FTC at bay.

Not surprisingly, the settlement also recognizes that third-parties, whether vendors or franchisees, are often the weakest link in data security. The *Wyndham* settlement essentially requires that firewalls or barriers be placed between Wyndham's corporate servers and those of its franchisees. This suggests that the Commission will be focused on how organizations deal with third-parties outside their own corporate network and the safeguards needed to do so effectively.

While the *Wyndham* settlement foreclosed the possibility that a federal court would for the first time weigh in on whether the agency's allegations met the consumer harm threshold under Section 5, the *LabMD* case might provide an opportunity to revisit that issue. The ALJ's ruling in *LabMD* held that Section 5's unfairness prong will generally require ''proof of actual consumer harm and that ''[s]ubjective feelings of harm, such as embarrassment, upset or stigma, standing alone, without accompanying, clearly demonstrated tangible injury, do not constitute 'substantial injury' '' within the meaning of Section 5.

Not surprisingly, the settlement also recognizes that third-parties, whether vendors or franchisees, are often the weakest link in data security.

Courts have struggled with the question of what constitutes sufficient injury to satisfy jurisdictional considerations because Article III requires a showing of injury-in-fact to satisfy the Constitution's requirements of an actual ''case'' or ''controversy.'' It remains unclear how questions of injury will be resolved in the data breach context especially in light of the U.S. Supreme Court's current consideration of standing in *Spokeo, Inc. v. Robins*.[28]

Historically, federal agencies like the FTC have not been held to the same standard of demonstrating injury in order to enforce statutory mandates such as Section 5 of the FTC Act. The Commission has traditionally relied on a theory of increased risk or possibility of harm to show that an act or practice caused or was likely to cause substantial consumer injury. This favored status is now front and center in the current *LabMD* appeal. If LabMD has its way, the FTC will need to deal with ''injury'' as an element of its enforcement actions in the same way as a private plaintiff, which would raise the bar and the FTC's burden in pursuing future data security enforcement actions.

[28] The U.S. Supreme Court recently heard oral argument in *Spokeo, Inc. v. Robins*, Case No. 13-1339 (Nov. 2, 2015) (http://www.supremecourt.gov/oral_arguments/argument_transcripts/13-1339_6j36.pdf). On appeal in *Spokeo* is a ruling from the Ninth Circuit Court of Appeals that permitted plaintiff Thomas Robins to establish standing under the Fair Credit Reporting Act (FCRA) with a speculative injury. Spokeo, a data aggregator, allegedly posted false information about Robins' finances, marital status and educational background. In his lawsuit, Robins claimed these misrepresentations would negatively affect his credit, insurance and employment outlook. The Ninth Circuit found that, although Robins did not suffer actual damages, a statutory violation of the FCRA satisfied Article III's injury-in-fact requirement. (http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/13-1339.htm). The Supreme Court granted certiorari to determine ''whether Congress can create Article III standing . . . by authorizing a private right of action based on a bare statutory violation.'' (http://www.supremecourt.gov/qp/13-01339qp.pdf).