GIBBONS

JENNIFER A. HRADIL
Director

Gibbons P.C.
One Gateway Center
Newark, New Jersey 07102-5310
Direct: (973) 596-4495 Fax: (973) 639-6487
jhradil@gibbonslaw.com

February 6, 2014

VIA ECF

The Honorable Esther Salas, U.S.D.J.
United States District Court
District of New Jersey
50 Walnut Street
Newark, New Jersey 07102

Re: *Federal Trade Commission v. Wyndham Worldwide Corporation, et al.*
Civil Action No.: 13-1887 (ES) (JAD)

Dear Judge Salas:

This firm, along with Kirkland & Ellis LLP and Ropes & Gray LLP, represents Wyndham Worldwide Corporation, Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LLC, and Wyndham Hotel Management, Inc. (collectively, "Wyndham") in the above-referenced action. Wyndham respectfully writes to draw the Court's attention to two recent developments that bear on the pending motions to dismiss. Specifically, these developments (1) further support Wyndham's contention that the FTC has not provided Wyndham—or any other entity—with fair notice of what data-security protections a company must employ to comply with Section 5 of the FTC Act, and (2) undermine the FTC's position that it is not feasible to publish regulations and rules explaining what qualifies as "reasonable" data-security practices. Wyndham appreciates that this Court has allowed extensive briefing in this case. Wyndham, nonetheless, felt obliged to alert the Court of recent developments in Congress this week, which could not be referenced in prior submissions. Wyndham will not provide argument on these developments unless requested to do so by the Court.

First, on January 30, 2014, Senator John Rockefeller (D-WV) introduced the Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014) (attached as Exhibit A). Among other things, this bill requires the Federal Trade Commission to issue rules—after notice and comment—that require agencies and businesses "to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information taking into consideration" various factors, including "the current state of the art in administrative, technical, and physical safeguards for protecting such information." *Id.* § 2(a)(1). It also requires the FTC, in consultation with the National Institute of Standards and Technology, to issue rules—after notice and comment—that will "identify each security technology and methodology" that would render sensitive personally identifiable data "unusable, unreadable, or indecipherable." *Id.* § 3(g)(2)(A)(i), (3). The FTC must make these identifications in consultation "with relevant industries, consumer organizations, data security and identity theft prevention experts, and established standards setting bodies." *Id.* § 3(g)(3)(A).

Second, on February 3, 2014, Senator Richard Blumenthal (D-CT) introduced the Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014) (attached as Exhibit B). This bill, like S. 1976, requires the FTC, in consultation with the National Institute of Standards and Technology to issue rules—again, after notice-and-comment—"to identify security methodologies or technologies, such as encryption, which render sensitive personally identifiable information unusable, unreadable, or indecipherable." *Id.* § 212(b)(A)(2)(iii)(I). In promulgating these rules, S. 1995 would require the FTC to "consult with the relevant industries, consumer organizations, and data security and identity theft prevention experts and established standards setting bodies." *Id.* § 212(b)(A)(2)(iii)(II).

Wyndham believes that these provisions from the attached bills will assist the Court in rendering a decision on the pending motions to dismiss. We thank your Honor for your consideration of this submission. As noted above, Defendants will not provide any argument with respect to these developments unless the Court so requests.

Respectfully,

s/ Jennifer A. Hradil
Jennifer A. Hradil
Director

cc: All counsel of record (via ECF)