Wiley Rein LLP

1776 K STREET NW
WASHINGTON, DC 20006
PHONE 202.719.7000
FAX 202.719.7049

7925 JONES BRANCH DRIVE
McLEAN, VA 22102
PHONE 703.905.2800
FAX 703.905.2820

www.wileyrein.com

January 30, 2015

Bennett L. Ross
202.719.7524
bross@wileyrein.com

VIA ELECTRONIC FILING

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Re: *In the Matter of Petition of American Hotel & Lodging Association, Marriott International, Inc., and Ryman Hospitality Properties for a Declaratory Ruling to Interpret 47 U.S.C. § 333, or, in the Alternative, for Rulemaking;* RM 11737

Dear Ms. Dortch:

The American Hotel & Lodging Association, Marriott International, Inc., and Ryman Hospitality Properties (collectively, "Petitioners") respectfully withdraw their petition for declaratory ruling or, in the alternative, for rulemaking, in order to more quickly and comprehensively address some of the pressing security questions raised by Petitioners and to focus efforts on establishing the American Hotel & Lodging Association Cybersecurity Task Force.

Petitioners filed the petition in an attempt to obtain Commission guidance on important issues that affect all operators of Wireless Local Area Networks ("WLANs"). The petition was never intended to condone carte blanche blocking of personal Wi-Fi devices by WLAN operators, and the assertion that hotels have "intentionally block[ed] or disrupt[ed] personal Wi-Fi hot spots … to force consumers to purchase access to the property owner's Wi-Fi network" is false.[1] Indeed, Petitioners strongly supports – and partners with – technology companies to ensure that our guests' have access to the latest innovations.

Broad access to Wi-Fi is among the capabilities that Petitioners' guests demand. They also demand access to a safe and secure system in order to protect private information from criminals seeking to exploit consumers. As many Americans have experienced, cybersecurity attacks are more prevalent than ever before, with some 42 million cybersecurity incidents, targeting all types of organizations reported last year. This number represents a 50 percent increase over the year before – and is

---

1 FCC Enforcement Advisory, DA 15-113, at 2 (Jan. 27, 2015).

representative of the real and serious cybersecurity threat that businesses are grappling with as they work to protect consumer information.

The hospitality industry felt compelled to raise this pressing issue with the FCC. Of particular concern to the hospitality industry is the ability of a hotel to protect the security of its network and guests by using wireless intrusion detection and prevention systems that are part of WLAN equipment authorized by the FCC. These systems are employed by numerous WLAN operators across multiple industries, including the federal government.

Indeed, the Department of Homeland Security released a technical reference in September 2011 entitled "Wireless Local Area Network (WLAN) Reference Architecture," which was "the product of an ongoing multi-agency collaboration to provide additional guidance for the successful implementation of [WLANs] at Federal civilian agencies." In this document, DHS requires that internal WLANs operated by federal agencies use wireless intrusion detection and prevention systems and "recommends" the use of such systems by authorized visitor WLANs.

To be sure, DHS is primarily tasked with ensuring the "security and resiliency" of the federal government's networks. However, DHS also provides "assistance to the private sector" because, according to DHS, "efforts to secure their own cyber networks help the nation's overall cybersecurity posture."[2] Indeed, DHS' guidance on the use of wireless intrusion detection and prevention systems is a core requirement imposed by the credit card companies on every merchant that processes credit cards in a wireless environment.

Petitioners believe that very real threats still exists, and therefore the hospitality industry is moving forward and establishing an industry task force that will partner with experts and leaders in the technology sector to find and implement the most effective market-based solutions available to tackle growing cyber threats. Hotels have a responsibility to their customers to ensure they have both access to Wi-Fi and a secure network. The hospitality industry commits to working aggressively to

---

2 http://www.dhs.gov/secure-cyber-networks.

develop recommendations and find solutions that balance the need to protect guest information and offer wide availability of wireless connectivity.

Sincerely yours,

Bennett L. Ross/tp

Bennett L. Ross

BLR:tp