

**Before the
Federal Communications Commission
Washington, DC 20554**

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

To: Chief, Consumer & Governmental Affairs Bureau

COMMENTS OF SMART CITY NETWORKS, LP

Mark Haley
President
SMART CITY NETWORKS, LP
5795 W. Badura Ave., Suite 110
Las Vegas, NV 89118
(702) 943-6000

December 19, 2014

TABLE OF CONTENTS

I.	INTRODUCTION	2
II.	MANAGEMENT OF THE WI-FI ENVIRONMENT IS CRITICAL FOR MANY INDUSTRIES THROUGHOUT THE NATION	4
III.	SECTION 333 DOES NOT APPLY TO DE-AUTHENTICATION BETWEEN UNLICENSED DEVICES.....	7
IV.	DE-AUTHENTICATION CAN BE A REASONABLE PRACTICE TO PROVIDE A WELL MANAGED WI-FI ENVIRONMENT WHERE IT IS NEEDED MOST	12
	CONCLUSION.....	14

SUMMARY

Smart City urges the Commission to take this opportunity to make clear that the operation of Commission-authorized equipment by a Wi-Fi operator in managing its network, on its own premises and for private events like conventions, does not violate Section 333 of the Communications Act of 1934. Wi-Fi has evolved far beyond a public convenience. Billions of dollars in business is conducted and concluded each year during convention events. Reliable, high quality Wi-Fi service can mean the difference between success and failure for the companies participating in the show and for the venues hosting the show. Convention exhibitors depend upon the availability of Wi-Fi to demonstrate and control products ranging from robotic and household appliances to medical devices and manufacturing equipment. Actual business transactions are being conducted wirelessly more and more in these venues, as well. Under such circumstances, convention exhibitors and attendees have reasonably come to expect that the Wi-Fi network supplied by the venue specifically for each event will work.

Reasonable network management is critical to meet this expectation. Without a managed Wi-Fi airspace during convention events, many exhibitors would be unable to reliably conduct their business and demonstrate their products. Billions of dollars in business could be lost and cities or venues could lose substantial convention business along with the millions of jobs supported by these events and the tourism associated with these events.

De-authentication technology, which is well-understood and has been endorsed by the U.S. Department of Commerce and U.S. Department of Defense, can be an important element of managing Wi-Fi networks deployed in high-density settings, such as convention centers. Indeed, the practice is wide-spread among airports, governments, colleges and universities, and hospitals – essentially any entity or institution that deploys a Wi-Fi network to support multiple users simultaneously in high-density RF environments.

Moreover, de-authentication technology is *not* signal jamming. Signal jammers are unlawful devices that transmit powerful radio signals that overpower, jam, or interfere with licensed communications. De-authentication, by contrast, involves the termination (often very temporary) of connections either between a rogue or misconfigured wireless endpoint device and an authorized access point or between an unauthorized wireless endpoint device and a rogue or misconfigured access point by sending messages to the endpoints, telling them to de-associate the current session. In addition, de-authentication is built into *lawful* Wi-Fi devices and networks systems that operate in the unlicensed 2.4 and 5 GHz spectrum bands in accordance with IEEE 802.11 standards and are manufactured and sold pursuant to the Commission's equipment authorization rules.

Under these circumstances, the Commission should explicitly acknowledge that Section 333 does not prohibit a Wi-Fi network operator from managing its own network on its own premises. If, however, the Commission cannot issue such a declaration, it should initiate a rulemaking to amend its rules to provide guidance with respect to how de-authentication may be used consistent with Section 333. In this regard, the Commission should consider permitting de-authentication based on the Relative Signal Strength Indicator (“RSSI”) level of an unauthorized access point or wireless device. De-authentication based on RSSI levels would target only those access points and wireless devices that may very well threaten the widespread availability and

reliability of Wi-Fi networks in high-density environments such as convention exhibit halls. Under a reasonable RSSI-based standard, de-authentication would protect the broad community of Wi-Fi users in these environments in a targeted, objective and neutral way, thereby serving the critical goal of maintaining the secure and reliable availability of Wi-Fi networks.

**Before the
Federal Communications Commission
Washington, DC 20554**

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

COMMENTS OF SMART CITY NETWORKS, LP

Smart City Networks, LP (“Smart City”)¹ submits these comments in support of the above-captioned petition for declaratory ruling.² The Commission should take this opportunity to make clear that the operation of Commission-authorized equipment by a Wi-Fi operator in managing its network, on its own premises and during conventions and other such private events, does not violate Section 333 of the Communications Act of 1934 (the “Act”), as amended, 47 U.S.C. § 333 (“Section 333”).³ If the Commission concludes, however, that it should regulate interference to Wi-Fi and other unlicensed Part 15 devices, it should initiate a rulemaking to develop parameters that will permit Wi-Fi network management while protecting against interference consistent with Section 333.

¹ Smart City provides technology and telecommunications services for the meeting and convention industry. The growth of the Internet and wireless products and services places an ever increasing emphasis on the need for technology solutions in convention centers. Cities, convention centers, tradeshows, exhibitors and attendees all have a common interest in ensuring a wireless environment that operates for the benefit of the overall ecosystem and Smart City contracts with the various convention venues to deliver high quality, secure, and reliable Wi-Fi service to the centers and their end-user exhibitors.

² Petition for Declaratory Ruling or, In the Alternative, For Rulemaking (filed by the American Hospitality & Lodging Association, Marriott International, Inc., and Ryman Hospitality Properties on Aug. 25, 2014 (“Petition”). See Public Notice, “Consumer & Governmental Affairs Bureau Reference Information Center, Petition for Rulemaking Filed,” Rep. No. 3012 (rel. Nov. 19, 2014).

³ Petition at 1.

I. INTRODUCTION

In our evolving interconnected world, secure and reliable wireless networks serve an increasingly important role as part of our Nation's economic engine, supporting the creation of new business opportunities throughout America. The expanding use of Wi-Fi networks to conduct business at conventions and tradeshow is a clear example of this trend. Wi-Fi has evolved far beyond a public convenience to the point where businesses and governments expect that Wi-Fi networks provided for their use in a closed campus setting and for private events will work. Indeed, in the context of convention centers, billions of dollars in business can hinge on the ability to rely upon the Wi-Fi service provided by the venue. Convention exhibitors routinely depend upon the secure, reliable wireless Internet connectivity that Wi-Fi enables to demonstrate and control products ranging from robotic and household appliances to medical devices and manufacturing equipment. The functioning of a convention center's Wi-Fi network could be the difference between success and failure for the companies participating in a tradeshow and for the venue hosting the show. Without a managed Wi-Fi airspace during convention events, many exhibitors simply would be unable to reliably conduct their business and demonstrate their products.

De-authentication technology can be an important element of managing Wi-Fi networks deployed in high-density settings, such as convention centers.⁴ The practice is wide-spread, well-understood, and has been endorsed by agencies of the federal government. For instance, the

⁴ As the National Institute of Standards and Technology ("NIST") describes it, de-authentication technologies "detect attacks, misconfigurations, and policy violations at the [Wireless Local Area Network] protocol level." National Institute of Standards and Technology, "Guide To Intrusion Detection and Prevention Systems (IDPS), Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-94, at 5-8 (Feb. 2007) ("NIST Recommendations"). It can also "identify the physical location of a detected threat by using *triangulation* – estimating the threat's approximate distance from multiple sensors by the strength of the threat's signal received by each sensor, then calculating the physical location at which the threat would be the estimated distance from each sensor." *Id.* at 5-9.

United States Department of Defense (“DoD”) mandates the use of network management and de-authentication technology in connection with its owned and operated networks.⁵ Likewise, NIST, part of the United States Department of Commerce, in implementing the Federal Information Security Management Act of 2002, has recommended the use of de-authentication technologies for all federal agencies and has provided guidance for “designing, implementing, configuring, securing, monitoring, and maintaining” such technology.⁶ The NIST Recommendations also state that its guidance “may be used by nongovernmental agencies on a voluntary basis.”⁷

For its part, the Commission itself has given no previous indication that the use of de-authentication technology is prohibited.⁸ To the contrary, such technology would appear to be entirely legal. It is built into Wi-Fi devices and networks systems that operate in the unlicensed 2.4 and 5 GHz spectrum bands in accordance with Institute of Electrical Electronics Engineers (“IEEE”) 802.11 standards and are manufactured and sold pursuant to the Commission’s equipment authorization rules.⁹

⁵ DoD, Instruction, “Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies,” Number 8420.01, Enclosure 3, p. 17 (Nov. 3, 2009).

⁶ NIST Recommendations at 1-1.

⁷ *Id.*

⁸ The Commission’s October 17, 2012 Cybersecurity Awareness Expo featured a speaker covering the NIST Recommendations. See FCC, Event, “Cybersecurity Awareness Expo” (Oct. 17, 2012), available at <http://www.fcc.gov/events/cybersecurity-awareness-expo>; see also, AirTight Networks, Press Release, “AirTight Presents – Understanding the GAO NIST Guidelines on Wireless Security – at FCC Security Awareness Day” (Oct. 11, 2012), available at http://www.airtightnetworks.com/home/news/pr/select_category/34/article/123/airtight-presents-understanding-the-gao-nist-guidelines-on-wireless-security-at-fcc-security-awa.html. To the best of Smart City’s knowledge, however, the Commission gave no indication at this event that de-authentication is unlawful.

⁹ 47 C.F.R. §§ 2.803, 2.901, 15.201(b).

Given this tacit support for de-authentication at the federal level, many industries and entities that deploy Wi-Fi networks to support multiple users simultaneously in high-density environments now rely upon de-authentication and other tools to manage their networks. Hospitals for instance use de-authentication and other tools to manage their Wi-Fi networks in order to maintain connectivity for life-critical devices and well as to ensure compliance with the requirements of the Health Information Portability and Accountability Act (“HIPAA”). Colleges and universities also rely on de-authentication and other tools to manage their own Wi-Fi networks.

A Commission interpretation of Section 333 that would render de-authentication unlawful would be poor public policy. Moreover, neither the Act itself nor the Commission’s rules would support such a reading, and any such reading would seriously undermine decades of Commission policy and rules, which have permitted deployment of a staggering array of unlicensed devices providing countless benefits to the American people.

II. MANAGEMENT OF THE WI-FI ENVIRONMENT IS CRITICAL FOR MANY INDUSTRIES THROUGHOUT THE NATION

We live in an age in which more and more data is being transmitted through Wi-Fi networks.¹⁰ On one hand, entities such as convention centers, airports, government offices, universities, and hospitals, around the world are increasingly deploying Wi-Fi networks that are designed for use in high-density environments and that can support thousands of users simultaneously. At the same time, individuals utilizing these venues are carrying, on average, three devices that can serve as Wi-Fi transmitters, e.g., smartphones, tablets, and laptop

¹⁰ “By 2018, wired networks will account for 39 percent of IP traffic, *while Wi-Fi and mobile networks will account for 61 percent of IP traffic.*” Cisco, “The Zettabyte Era: Trends and Analysis,” (June 10, 2014) (emphasis added) (“Zettabyte White Paper”), available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.

computers. The interaction of Wi-Fi transmitters operated by transient visitors in areas where Wi-Fi networks are deployed can give rise to crippling interference resulting in reduced throughput and quality of service for all users. Moreover, transient or unauthorized Wi-Fi transmitters can serve as easy-to-deploy platforms for launching a variety of attacks that threaten the security of Wi-Fi networks, including attacks such as man-in-the-middle, Address Resolution Protocol poisoning, DHCP/DNS hijacking, and injection of network worms and viruses.¹¹

Given these facts, failure to manage Wi-Fi networks can have serious economic consequences. One of the best examples of a failed wireless event is Steve Jobs' attempted demonstration of the new iPhone 4 when it was launched in June of 2010 in San Francisco.¹² The failure of this demonstration garnered major media attention and was very quickly communicated via social media and other news outlets. In fact, the YouTube video of the iPhone 4 failure has been viewed almost 1.5 million times. A reputation for having unreliable technology that could expose convention goes to such failures could result in a convention center losing a major tradeshow or in a conference not returning to that venue on an annual basis. Worse, a venue's reputation can be damaged to the point that shows would not even consider bringing their events to that city or facility, which could ultimately cause the loss of thousands of jobs.

Therefore, it is indisputable that Wi-Fi networks must be managed to prevent unauthorized Wi-Fi transmitters from causing interference that can reduce throughput and quality of service for the vast majority of users. To guard against these harms, Wi-Fi network management tools like de-authentication are widespread across the nation – in fact, across the

¹¹ See Petition at 7.

¹² See <https://www.youtube.com/watch?v=znxQOPFg2mo>.

globe. International venue managers from Canada and Europe attending the Association Internationale des Palais de Congress (<http://www.aipc.org/>) in Berlin in July of 2014 confirmed the widespread use of containment features to control their venue's wireless environments.

In addition to commercially critical environments such as convention centers, Wi-Fi network management and de-authentication supports mission-critical and life-critical applications provided in airports, government facilities, and hospitals, as well as at universities and other institutions. In order to meet the unique challenges of the hospital environment and satisfy the absolute priority of maintaining connectivity for life-critical devices and ensure compliance with HIPAA requirements, hospitals likewise must manage their Wi-Fi environments.¹³ The utilization of de-authentication technology is now included among the best practices for managing Wi-Fi networks in the difficult environments of hospitals.¹⁴ Furthermore, Wi-Fi management tools are commonly used to manage Wi-Fi networks on our nation's college campuses,¹⁵ and as noted above, our federal government has given its stamp of approval to the use of de-authentication.¹⁶

¹³ Cf. Jeff Rowe, "Wi-Fi in Hospitals: A Moving Target," HealthCareIT News (Nov. 25, 2013) available at <http://www.healthcareitnews.com/print/72546>; Carousel Industries, Podcast, "Challenges and Benefits of Wi-Fi and Wireless Networking in Hospitals" (May 15, 2013) available at <http://blogs.carouselindustries.com/wireless/challenges-and-benefits-of-wifi-and-wireless-networking-in-hospitals>. See also Robert Chilton, TechKnowledge Corporation, "Can Your Wireless Network Handle EMR Needs?," (Feb. 14, 2011) available at <http://www.hhmglobal.com/knowledge-bank/articles/can-your-wireless-network-handle-emr-needs> (marked advances in Wi-Fi networks include the fact that controllers that can "detect unauthorized users and unauthorized Access points" have helped make it possible for hospitals to establish strong, secure wireless networks).

¹⁴ See Aerohive Networks, Compliance Whitepaper, "Wireless LAN Best Practices for Compliant Care," at 9-10 (2013) available at <http://www.aerohive.com/pdfs/Aerohive-Whitepaper-HIPAA-Compliance.pdf>; Aerohive Service Level Assurance, Wireless Fidelity Achieved (2011) available at http://www.aerohive.com/pdfs/Aerohive-Whitepaper-Service_Level_Assurance.pdf; Meru Networks, "Meru Uninterrupted Care Network, An Architecture Overview," Wireless Networks Designed for Hospitals (May 2013).

¹⁵ Petition at 10-11.

¹⁶ See *supra* notes 4-6.

It also bears emphasizing that de-authentication technology is separate and distinct from signal jamming. Signal jammers are unlawful devices that transmit powerful radio signals that overpower, jam, or interfere with authorized communications.¹⁷ De-authentication, by contrast, is not the transmission of powerful radio signals to overpower, jam, or interfere with authorized communications. De-authentication involves the termination of connections either between a rogue or misconfigured wireless endpoint device and an authorized access point or between an unauthorized wireless endpoint device and a rogue or misconfigured access point by sending messages to the endpoints, telling them to deassociate the current session.¹⁸ In addition, de-authentication is built into *lawful* Wi-Fi devices and networks systems that operate in the unlicensed 2.4 and 5 GHz spectrum bands in accordance with IEEE 802.11 standards and are manufactured and sold pursuant to the Commission's equipment authorization rules.

Therefore, the use of de-authentication does not portend interference to licensed spectrum or spectrum used by the federal government. Rather, de-authentication involves unlicensed Wi-Fi technology, lawfully manufactured and marketed, used by Wi-Fi network operators to manage their networks in high-density environments. Nothing in Section 333 of the Act precludes this practice. To the contrary, as shown below, Section 333 simply does not apply to Wi-Fi network operations or prohibit interference to unlicensed devices.

III. SECTION 333 DOES NOT APPLY TO DE-AUTHENTICATION BETWEEN UNLICENSED DEVICES

Section 333 of the Act does not protect Part 15 devices from interference. Section 333 provides:

¹⁷ See *Office of Engineering and Technology Compliance and Information Bureau Warn Against the Manufacture, Importation, Marketing or Operation of Transmitters Designed to Prevent or Otherwise Interfere with Cellular Radio Communications*, 15 FCC Rcd 6997 (OET 1999).

¹⁸ NIST Recommendations at 5-11.

No person shall willfully or maliciously interfere with or cause interference to any radio communications of *any station* licensed or authorized by or under this Act or operated by the United States Government.¹⁹

In short, Section 333 protects only “stations.” A careful reading of the Act and the Commission’s rules reveals that the term “station” as used in Section 333 does not extend to Part 15 devices.

The Act does not provide a clear or useful definition of the term “station.” “The term ‘radio station’ or ‘station’” is defined to mean “*a station* equipped to engage in radio communication or radio transmission of energy.”²⁰ In other words, for equipment to be defined as a “station” it must be a “station.” The logical circularity of this definition renders it virtually useless for analytic purposes. Further, the Act provides no definition of the term “device.” Thus, one must look to the remainder of the Act to determine whether a Part 15 device constitutes a “station” for purposes of Section 333.

An examination of other provisions of Title III of the Act makes it readily apparent that a Part 15 device is not a “station” for purposes of Section 333 or other provisions of Title III. For example, Sections 307 and 308 set out the requirements for “station” applications, licenses, modifications, and renewals.²¹ Section 309 establishes processes for Commission action on applications for a “station” license, modification, or renewal under Section 308.²² Section 310 includes certain ownership limitations on, and requirements for the assignment of and transfer of control of, “station licenses.”²³ The Commission has never applied the requirements of these

¹⁹ 47 U.S.C. § 333 (emphasis added).

²⁰ *Id.* § 153(42) (emphasis added).

²¹ *Id.* §§ 307, 308.

²² *Id.* § 309.

²³ *Id.* § 310.

sections to Part 15 devices. Thus, for example, the Commission has never suggested that applications for Part 15 device authorization cannot be denied without a hearing, that Part 15 authorizations cannot be transferred without prior Commission approval, or that Part 15 authorizations cannot be granted to foreign government or their representatives.

In fact, the Commission’s statutory authority over the interference potential of unlicensed wireless devices is entirely separate and distinct from the Title III provisions governing interference between “radio stations” or “stations.” Section 302 of the Act provides in pertinent part:

The Commission may, consistent with the public interest, convenience, and necessity, *make reasonable regulations (1) governing the interference potential of devices* which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications²⁴

Logic dictates that Section 302 and the Commission’s authority to regulate interference under that provision must necessarily be distinct from the Commission’s authority to regulate interference “between stations” under Section 303(f)²⁵ If Part 15 “devices” authorized under Section 302 were “stations” for purposes of Section 303(f), then Section 302, which authorizes the Commission to regulate “the interference potential of devices,” would be superfluous. Section 302 must have been designed to give Commission authority that the agency did not already have.

Commission rules reflect this reality. The Commission’s Part 15 rules set out the “regulations under which an intentional, unintentional, or incidental radiator may be operated

²⁴ *Id.* § 302a(a)(1) (emphasis supplied). *See also id.* § 302a(b), (c), & (e) (all referring to “devices,” not stations).

²⁵ *Id.* §303(f).

without an individual license.”²⁶ These rules govern a wide array of “devices” but do not cover “radio stations” or “stations.”²⁷ With the sole exception of CB “stations,” which are exempt from licensing requirements under Section 307(e) of the Act, the Part 15 rules do not purport to regulate any “radio station” or “station.”²⁸

The Part 15 rules governing interference further demonstrate that Part 15 devices are subject to a regulatory regime that is separate and distinct from Section 333. Specifically, Part 15 subjects the operation of unlicensed devices “to the conditions that no *harmful interference* is caused and that *interference* must be accepted that may be caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.”²⁹ The term “harmful interference” refers to the disruption of a “radiocommunications service” and Wi-Fi service is not a “radiocommunications service.”³⁰ Thus, as the Commission’s own Office of Engineering and Technology has put it: “*interference caused to a Part 15 device by another Part 15 device does not constitute harmful interference.*”³¹ Thus, sending a de-authentication packet to a Part 15 device cannot be construed as harmful interference under this rule.

²⁶ 47 C.F.R. § 15.1(a).

²⁷ See, e.g., *id.* § 15.3(a) (auditory assistance devices); 15.3(b) (biomedical telemetry devices); 15.3(c) (cable system terminal devices); 15.3(h) (Class A digital devices); 15.3(i) (Class B digital devices); 15.3(k) (digital devices); 15.3(r) (peripheral devices).

²⁸ *Id.* § 15.3(g).

²⁹ *Id.* § 15.5(b) (emphasis added).

³⁰ See 47 C.F.R. § 15.3(m) (Harmful interference is “[a]ny emission, radiation or induction that endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunications service operating in accordance with this chapter.”); *id.* § 2.1 (A radiocommunications service is “[a] service as defined in this Section involving the transmission, emission and/or reception of radio waves for specific telecommunication purposes.”).

³¹ *Revision of Part 15 of the Commission’s Rules Regarding Ultra-Wideband Transmission Systems*, 17 FCC Rcd 13522, 13524 n.7 (OET 2002) (emphasis added).

Likewise, if a Part 15 device were a “radio station” or “station” protected by Section 333, then the rule’s requirement that these devices accept “interference” would contravene the protections established in Section 333 of the Act. It cannot be the case that a Part 15 device is both unprotected against interference under Part 15 and protected against interference under Section 333 of the Act.

In short, the only reasonable way to read Section 302 of the Act and Part 15 of the Commission’s rules together with Section 333 and the other provisions of Title III of the Act is to acknowledge that “radio stations” or “stations” are separate and distinct from Part 15 wireless devices, and that therefore Section 333 does not apply to the latter. To do otherwise would be inconsistent with decades of Commission policy and rules implementing a part 15 regulatory regime that permits a staggering array of unlicensed devices that provide countless benefits to the American people.

An expansive reading of Section 333 as covering Part 15 devices would also conflict with the fundamental policies underlying the Commission’s OTARD rules. The OTARD rules prohibit restrictions on property that impair the use of certain antennas that are located on property within the exclusive use or control of the antenna user where the user has a direct or indirect ownership or leasehold in the property.”³² Reading Section 333 as prohibiting Wi-Fi operators from protecting against unauthorized access points on their networks, located on their premises, would have the incongruous result of allowing third parties, with no ownership or leasehold interest, to restrict an operator’s use of its network. The Commission, therefore, should grant the Petition and declare that Section 333 does not prohibit Wi-Fi network operators from using de-authentication to manage their networks on their own premises.

³² 47 C.F.R. § 1.4000; *Continental Airlines Petition for Declaratory Ruling Regarding the Over-the-Air Reception Devices (OTARD) Rules*, 21 FCC Rcd 13201, 13206 ¶ 12 (2006).

IV. DE-AUTHENTICATION CAN BE A REASONABLE PRACTICE TO PROVIDE A WELL MANAGED WI-FI ENVIRONMENT WHERE IT IS NEEDED MOST

Should the Commission conclude that it cannot issue the declaration requested by the Petition, it should initiate a rulemaking to amend its rules to provide guidance with respect to how de-authentication may be used consistent with Section 333. A rulemaking not only would be required as a legal and procedural matter,³³ but also would allow the Commission to gather information from network operators about the reasonable use of de-authentication in real world situations.

In this regard, Smart City submits that its use of de-authentication in convention venues might serve the Commission as an example of how de-authentication can be used in a way that reasonably balances the needs to network management with the use of third party and mobile devices in high-density environments. Smart City has not used de-authentication in the majority of the convention venues that it serves and, in light of the recent Order and Consent Decree in the Marriott case,³⁴ it has discontinued the use of de-authentication in those venues where it did use this technology.

In most instances where it did use de-authentication, however, Smart City used the Relative Signal Strength Indicator (“RSSI”) level as the criterion for identifying and containing unauthorized access points that posed an imminent threat to the security and/or reliability of the Wi-Fi environment. Specifically, Smart City created a custom rule in the wireless protection policies built into the wireless controllers it uses. Targeting access points and wireless devices located in the exhibit halls, where interference and noise levels are the greatest, the wireless controllers identified as “Unclassified” those access points and wireless devices that were not

³³ See Petition at 19-21.

³⁴ *Marriott International, Inc. and Marriott Hotel Services, Inc.*, Order and Consent Decree, File No. EB-IHD-13-00011303, DA 14-1444 (EB, rel. Oct. 3, 2014).

authorized by Smart City. Where an Unclassified access point or wireless device was found to have an RSSI level sufficient to threaten the RF environment in an exhibit hall (e.g., -65 to -0), it was reclassified as “Malicious” and clients associated or attempting to associate to the access point or wireless device were sent de-authentication packets if resources were available for containment. If no resources were available, the access points or wireless devices classified as “Malicious” were given a status of “containment pending” and no de-authentication packets were sent until resources became available.

Once the RSSI level of an access point or wireless device classified as “Malicious” improved to -66 to -100 for instance (e.g., if the unauthorized access point reduced power or moved away from the network-authorized access point with which it was interfering), the wireless controller automatically returned that access point or wireless device to Unclassified status and the wireless controller would no longer de-authenticate that access point or wireless device, allowing it to connect to the Smart City network.

De-authenticating based on the RSSI level of an unauthorized access point or wireless device in this way is a fundamentally reasonable practice. De-authentication is targeted only to those access points and wireless devices that actually may impair the throughput and reliability of the Wi-Fi network in the exhibit hall.³⁵ Furthermore, de-authentication is targeted to those access points and devices located within the confined and proprietary space of the exhibit hall, areas of the convention center that are licensed for a private event involving the private assembly

³⁵ To protect their legitimate need to ensure a secure and reliable Wi-Fi environment for exhibitors, convention centers could choose to impose, as a condition of entry onto their property, a restriction prohibiting all Wi-Fi access points except for those operated by authorized contractors from connecting to electrical outlets in exhibit halls. That approach, which the FCC has no jurisdiction to regulate, would be more restrictive than the RSSI-based approach that Smart City has used, which is reasonably designed to target only actual threats posed by the use of unauthorized access points in highly congested RF environments.

