# PUBLICATION

## Marriott Fined $600,000 For Wi-Fi Jamming

**December 18, 2014**

On October 3, 2014, Marriott International entered into a consent decree with the Federal Communications Commission (FCC) where Marriott agreed to pay a $600,000 fine for jamming conference guests' Wi-Fi hotspots at the Gaylord Opryland in Nashville, Tennessee.

In the consent decree, Marriott acknowledged that "one or more of its employees used containment features of a Wi-Fi monitoring system at the Gaylord Opryland to prevent consumers from connecting to the Internet via their own personal Wi-Fi networks." While employees were using these containment features to block guests' personal Wi-Fi, the FCC says that Marriott was charging consumers, businesses and exhibitors in the conference center rates ranging from $250 to $1,000 per device to access Marriott's own Wi-Fi network.

Travis LeBlanc, chief of the FCC's enforcement bureau, stated that "Consumers who purchase cellular data plans should be able to use them without fear that their personal internet connection will be blocked by their hotel or conference center. It is unacceptable for any hotel to intentionally disable personal hotspots while also charging consumers and small businesses high fees to use the hotel's own Wi-Fi network."

When asked by the press to explain whether its actions were the result of a rogue employee or an official policy, Marriott offered the following explanation: "Marriott has a strong interest in ensuring that when our guests use our Wi-Fi service, they will be protected from rogue wireless hotspots that can cause degraded service, insidious cyber-attacks and identity theft. Like many other institutions and companies in a wide variety of industries, the Gaylord Opryland protected its Wi-Fi network by using FCC-authorized equipment provided by well-known, reputable manufacturers. We believe that the Gaylord Opryland's actions were lawful. We will continue to encourage the FCC to pursue a rulemaking in order to eliminate the ongoing confusion resulting from today's action and to assess the merits of its underlying policy."

Although it is not immediately apparent which Wi-Fi management system was in use at the Gaylord Opryland, Ruckus Wireless lists Marriott as one of several major hotel systems that employs Ruckus's Zoneflex Wi-fi Management System. Zoneflex, like similar products produced by Cisco, Aptilo, Meru Networks, Antamedia and Aruba Networks, has the capability to interfere with "rogue" network access points. In general, rogue devices are defined as those that share a network operator's Wi-Fi spectrum but are not managed by the Wi-Fi network operator.

Cisco's documentation on rogue device management notes that "Containment is a method of using over-the-air packets to temporarily interrupt service on a rogue device until it can physically be removed. Containment works by spoofing de-authenticated packets with the spoofed source address of the rogue AP so that any clients associated are kicked off." Essentially, this capability works like a distributed denial of service (DDoS) attack. DDoS attacks in other contexts were one of the original reasons for the creation of the Computer Fraud and Abuse Act (CFAA), and remain one of the chief sources of liability under that statute today. Cisco notes in its Wi-Fi management documentation that rogue containment "can have legal implications when launched against neighboring networks. Ensure that the rogue device is within your network and poses a security risk before you launch the containment."

The Marriott consent decree noted that Marriott's liability arose under Section 333 of the Communications Act of 1934, which prohibits "willful or malicious interference with radio network signals," which the FCC has interpreted to include Wi-Fi networks. The commission has made enforcement of Section 333 a top priority in recent years, particularly against manufacturers and users of jamming devices. Two years ago, the FCC set up a tip line for people to report the sale of any type of signal jammers. The potential penalties are severe, including a $16,000 per day fine for continuing violations; and up to $112,500 for a single violation, seizure of the jamming equipment and even possible imprisonment.

Given the FCC's enhanced enforcement, as well as the potential for heavy fines under Section 333 and civil suits under the CFAA, operators of Wi-Fi networks like those in hotels need to be especially careful balancing network security issues with ensuring that security measures do not interfere with neighboring networks, as Marriott's did. It very well may be that Marriott's position is correct and the FCC is overreaching its enforcement mandate. Even if that is true, however, such a position is not worth the risk of an adverse enforcement action or a CFAA lawsuit, which could be brought as a civil class action. Hotel Wi-Fi operators should work hand-in-hand with their software providers and attorneys to ensure that any rogue device containment avoids legal liability.