Avoiding Hotel Data Breaches With a Risk Assessment Audit™ – Lessons From the Marriott International “Glitch”

30 November 2018

Click here for the latest articles on Data Technology, Privacy & Security.

Data breaches are back in the news, and this time, it’s a well-known hotel industry player: Marriott International. The company announced today that unauthorized access to their systems going back several years has exposed the names and other personal details of over 500 million guests. For hoteliers, this situation can be avoided by using the Global Hospitality Group® Risk Assessment Audit™, a comprehensive tool that combines your internal resources with our expertise in analyzing your risk profile, both for compliance purposes and to create effective data security strategies.

Bob Braun, senior member of JMBM’s Global Hospitality Group® and Co-Chair of the Firm’s Cybersecurity & Privacy Group, sums up what Marriott is facing and what lessons other hotels can learn from this incident, below.

Not a Good Day for Marriott

by Bob Braun

It’s unlikely that anyone in the hospitality industry – perhaps anyone who watches the news – hasn’t heard about the data breach at Marriott. Marriott’s pre-eminent position in the hotel industry, and the very size of the breach, with an estimated 500 million individuals impacted (putting it second behind the Yahoo breach) make this noteworthy.

What Happened?

While some of the information is available, most of the details have yet to be filled in. However, there are some key takeaways that every hotel owner, operator and brand should consider:

- First, this breach dates back more than 4 years, to 2014, prior to Starwood’s acquisition by Marriott. This highlights a key problem with data breaches in general, and a particular problem for the hospitality industry: data breaches are difficult to discover, creating not a one-time problem, but a continuing issue. In this case, Marriott reported that the intruders encrypted information from the hacked database, possibly to avoid detection by any data-loss prevention tools when removing the stolen information from the company’s network, further complicating the discovery and analysis of the breach.
- Marriott’s statement also detailed the information that was compromised, which it said “includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest account information, date of birth, gender, arrival and departure information, reservation date and communication preferences.” The theft of this information raises the possibility of creating significant damage to individuals, and its ramifications will be felt for a long time.
- One concern that needs to be considered is that Marriott was aware of potential issues at Starwood. Just after Marriott’s acquisition of Starwood, Starwood disclosed a breach involving more than 50 properties. According to Starwood’s disclosure at the time, that earlier breach stretched back at least one year — to November 2014.
- As we have noted earlier, while the size of this breach is breathtaking, Marriott is not alone. Virtually every major hotel company (and many smaller brands) have been impacted by breaches. This highlights that hotel companies are an
attractive target, both for the vast amounts of information they collect, as well as systemic issues (multiple legacy systems, extensive use of vendors, and a variety of access points).

- There will be a significant cost to this breach, including both direct costs (including breach notification and remediation, responding to regulatory and private actions) as well as reputational costs, translating into potential loss of business. And hotel owners operating under Marriott brands will undoubtedly bear at least part of the cost, as Marriott implements new policies, procedures and systems, and as consumers reconsider the security of Marriott systems.

**Industry Challenges**

This breach comes at particularly sensitive time, as privacy laws in the United States and abroad are becoming increasingly strict. Marriott will have to report and consider its obligations not only under United States laws – which are fragmented, and will include virtually every state, as well as the federal government – but also the impact of the European Union General Data Privacy Regulation, which itself is enforced by a variety of data regulators. Beyond this, other countries – ranging from India to Canada to China and Russia – have varying regulatory schemes which Marriott must address.

**What Do Hoteliers Need to Do?**

The Marriott data breach, however it ultimately plays out, should be a wake-up call for the hospitality industry. Owners, operators and brands need to create effective and comprehensive policies, procedures and systems to address an increasingly dangerous data environment. Existing processes – often a patchwork of uncoordinated documents – simply will not work in today’s new environment, which demands attention not only to the ever-increasing sophistication of hackers, but also the adoption of new laws and regulations that impose greater responsibility, and impose greater potential liability, on the collection, retention and use of personal information.

The JMBM Global Hospitality Group has joined with the JMBM Cybersecurity and Privacy Group to offer a Risk Assessment Audit™ and cybersecurity protocols geared specifically to the hotel industry. The Risk Assessment Audit™ is a comprehensive tool that joins together your internal resources (including information technology, information security and corporate governance) with our expertise in analyzing your risk profile to create an inclusive suite of findings, recommendations and strategy, both for compliance purposes and to create effective data security practices. For more information, contact Bob Braun at 310-785-5331 or rbraun@jmbm.com.

**Bob Braun** is a Senior Member of JMBM’s Global Hospitality Group® and is Co-Chair of the Firm’s Cybersecurity & Privacy Group. Bob has more than 20 years experience in representing hotel owners and developers in their contracts, relationships and disputes with hotel managers, licensors, franchisors and brands, and has negotiated hundreds of hotel management and franchise agreements. His practice includes experience with virtually every significant hotel brand and manager. Bob also advises clients on condo hotel securities issues and many transactional matters, including entity formation, financing, and joint ventures, and works with companies on their data technology, privacy and security matters. These include software licensing, cloud computing, e-commerce, data processing and outsourcing agreements for the hospitality industry.

In addition, Bob is a frequent lecturer as an expert in technology, privacy and data security issues, and is one of only two
attorneys in the 2015 listing of SuperLawyers to be recognized for expertise in Information Technology. Bob is on the Advisory Board of the Information Systems Security Association, Los Angeles chapter, and a member of the International Association of Privacy Professionals. Contact Bob Braun at 310.785.5331 or rbraun@jmbm.com.

This is Jim Butler, author of www.HotelLawBlog.com and hotel lawyer, signing off. Please contact us if you would like to discuss any issues or development that affect your hotel interests. We would like to see if our experience might help you create value or avoid unnecessary pitfalls. Who’s your hotel lawyer?

Jim Butler is a founding partner of JMBM and JMBM’s Global Hospitality Group® which provides business and legal advice to hotel owners, developers and investors. This advice covers hotel purchase, sale, development, financing, franchise, management, labor & employment, litigation, ADA, IP, EB-5 matters and many other areas.

Jim is recognized as one of the top hotel lawyers in the world and has led the Global Hospitality Group® in more than $87 billion of hotel transactions and more than 3,900 hotel properties located around the globe.

Jim’s group has advised on more than 100 EB-5 projects, closed more than $1.5 billion of EB-5 financing, and sourced more than half of that for our clients.

Contact Jim at +1-310-201-3526 or JButler@jmbm.com