Hotel lawyer alert for hotel owners and operators: Newest FTC warning about hotel data security

10 January 2020

See how JMBM’s Global Hospitality Group® can help you.

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

Hotel data breaches can have significant financial and reputational impacts on a brand, as evidenced by Marriott’s $123 million GDPR fine. In the article below, Bob Braun, senior member of JMBM’s Global Hospitality Group® and Co-Chair of the Firm’s Cybersecurity & Privacy Group, outlines the critical importance of data security for the hospitality industry.

— Jim

Hotel Managers and Owners Be Warned – You are Responsible for Your Hotel’s Data Security

by

Bob Braun, Cybersecurity Lawyer

The FTC Speaks

On January 6, 2020, the Director of the FTC’s Consumer Protection Bureau published a blog post with changes to the FTC’s approach to its orders and settlements of data breach enforcement actions. One of the key elements of the report was a revision to the FTC’s routine enforcement practice to ensure that its remedial data security orders include greater specificity about compliance expectations for companies subject to enforcement action and for third-party assessors engaged to conduct FTC-mandated monitoring and audits of targeted companies’ data security practices.

Beyond greater detail guiding data security requirements, the blog post highlights that a core element of the FTC’s model for remedial orders is that senior management, on at least an annual basis, present the company’s written information security program to the board or other governing body for oversight and review, and that management certify to the FTC that the company has complied with data security obligations.

The Growing Role of Managers and Boards in Data Security

The decision by the FTC reflects a growing consensus about the roles and responsibilities of management and boards for the adequacy of enterprise programs to identify, evaluate, and manage data and information security risks. While this is not the first time boards of directors have been held accountable for the security practices of the companies they represent, it shows that this obligation has become mainstream and should be noted by all companies, whether they

The FTC’s endorsement of data security-related corporate governance approaches, safeguards, and third-party monitoring methods is likely to impact enforcement expectations of other regulators, whether state, federal or local, responsible for administering data security compliance and breach notification regulations.
Impact on Hotels

Hotels need to be particularly aware of these issues, since hospitality companies collect enormous amounts of personal information, and have regularly been implicated in data breaches. As we have written before, hotels depend not just on location, price and amenities – they depend on the trust of their guests. Currently, the responsibility for the protection of personal data – guest data – is a hot potato. Owners, managers and brands need to work together to create a secure data environment or risk losing trust, and market share.

The CCPA Speaks

The stakes in this battle have been raised with the introduction of California’s Consumer Privacy Act which, among other things, requires businesses subject to the Act (which probably includes most hotel chains and larger hotels in California) to implement reasonable security standards, and authorizes individuals to bring private rights of action in the case of a data breach where an individual can show that the reasonableness standard was not met. Most importantly, the CCPA provides for damages of between $250 and $750 for each violation. Given that the number of impacted records in even a modest data breach reach into the thousands, the stakes for failure to take data security seriously have been raised.

What Should You Do?

In its 2016 California Data Breach Report, the California Attorney General included an appendix that sets out in detail the information security framework endorsed by the Attorney General, and it remains one of the few frameworks that sets out what a standard for a minimum level of information security. The report goes on to state that: “The 20 controls in the Center for Internet Security’s Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.”

All companies, and hotels in particular, should pay close attention to this standard. It is likely that in Attorney General regulatory action or private right of action initiated after a breach, a crucial inquiry will be directed at what kind of information security framework was in place, was it appropriate for the organization, was it being followed, and did the highest levels of management address the framework.

The JMBM Global Hospitality Group, in conjunction with the JMBM Cybersecurity and Privacy Group, work together to provide seamless and custom security frameworks that address the unique needs of hospitality companies. For more information, contact Robert Braun, rbraun@jmbm.com.

Further information about cybersecurity issues

If this article was of interest, you may also wish to read other articles by Bob Braun on “Data Technology, Privacy & Security,” which include the following:

The California Consumer Privacy Act – What Hoteliers Need to Know Now
Avoiding Hotel Data Breaches With a Risk Assessment Audit™ – Lessons From the Marriott International “Glitch”

California Adopts the California Consumer Privacy Act of 2018

GDPR: What you need to know about the EEU’s new data privacy rules

Cyberattacks on Hotels — What Should Hotel Owners and Operators Do?

Hotel Cybersecurity: Protecting your guests and your property from vendor data breaches

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 founding partner of JMBM and JMBM’s Global Hospitality Group®. We provide business and legal advice to hotel owners, developers, independent operators and investors. This advice covers critical hotel issues such as hotel purchase, sale, development, financing, franchise, management, ADA, and IP matters. We also have compelling experience in hotel litigation, union avoidance and union negotiations, and cybersecurity & data privacy.

JMBM’s Global Hospitality Group® has been involved in more than $87 billion of hotel transactions and more than 3,900 hotel properties located around the globe. Contact me at +1-310-201-3526 or jbutler@jmbm.com to discuss how we can help.

How can we help? Brochure Credentials Photo Gallery