Hotel Liability for Guest Information — What you need to know and how to avoid liability.

7 October 2012

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

Hotel Lawyer on hotels' liability for failure to protect hotel guests personal identities

My partner Robert Braun advises hotel owners in a wide range of operational issues, including information management. Because of the ubiquitous use of credit cards by hotel guests during a stay, as well as the growing demand for WiFi availability, hotels have been increasingly targeted by identity thieves. In his article below, Bob explains how hotels' liability for this new type of guest security has grown and what hotels can do to protect their guests' identities.

Hotel Liability for Guest Information and Identity
What you need to know
by
Robert E. Braun | Hotel Lawyer
A version of this article was first published in the September 21, 2012 issue of Hotel Business and is reprinted with permission.

Not too long ago, keeping guest information safe was a fairly straightforward process – perhaps the most innovative development was providing an in-room safe for valuables. This approach made sense at the time, when guest security was a matter of securing people and their physical possessions.

The industry now recognizes that hotel guests have valuables to protect that go far beyond watches and wallets, or even laptops and iPads – perhaps the most valuable information a hotel guest has is his or her identity, and unless a hotel actively safeguards it, those valuables are at risk. The ubiquity of credit card, wireless internet and other options, while essential to hotel operations, is also a source of insecurity.

Hotels are Targets

Hotels are obvious targets for identity and financial theft for many reasons. Hotels transact business through credit cards, and those credit cards are kept on file and can be accessed multiple times during a guest’s stay. The possibility that a credit card charge will be recorded occurs with each night’s room charge, room service, bar or restaurant bill, spa charge, and so on. Every charge is another opportunity for an identity thief to access the information using sophisticated computer hacks and other malicious software, generally without the hotel’s knowledge.

The need to respond to guest demands is another source of insecurity. The Identity Theft Resource Center noted, “The ability to connect to the Internet is an integral part of many individuals daily life. This has led to the increased demand for public WiFi.” As a result, hotels find themselves compelled to offer wireless internet, and that service is almost always unsecured. But an unsecured wireless network is “just as dangerous as leaving files of your most important personal
documents on a street curb for all to see. Hackers can easily get into an unsecured wireless network and get financial information, business records or sensitive e-mails." (PC World, ) “Got Wireless Security”. At the same time, hotels have little say in the matter. Guests demand wireless internet service.

Finally, hotels have employees — lots of employees — and many of them have access to the credit card and other personal information of guests. No matter how well trained and supervised, more personnel correlates to greater risk. The fact that low-level employees typically have access to key guest information, and that there is, historically, a high turnover in hotel employees, exacerbates the problem.

Some security researchers have described a wave of attacks against the hospitality industry. In 2010, the cybersecurity consultant Trustwave found that in 38% of its investigations, hotels and resorts were the victims of successful cyber intrusions, despite those firms only representing 3% of its customers. Hotels represent a disproportionate number of security breaches.

The Wyndham Case

In June 2012, the Federal Trade Commission filed a lawsuit against Wyndham hotels, claiming Wyndham misrepresented its security measures to prevent intrusions by computer hackers. In its press release, the FTC claimed Wyndham had subjected consumers’ data to an “unfair and deceptive” lack of protection that led to a series of breaches of Wyndham hotels and those of three subsidiaries. The lawsuit describes three attacks on the hotel chain and its franchisees beginning in 2008 that first compromised 500,000 credit card numbers stored by the firm, followed by attacks that breached another 50,000 and 69,000 accounts at other locations.

Key to the FTC complaint is its claim Wyndham failed to take common and well-known security measures. The FTC noted that Wyndham failed to require complex passwords, implemented a network setup that did not separate corporate and hotel systems, and used “improper software configurations” that led to sensitive payment card information being stored without encryption. The FTC complaint compared those failures to Wyndham’s privacy policy, which said that Wyndham strove to “recognize the importance of protecting the privacy of individual-specific (personally identifiable) information collected about guests, callers to our central reservation centers, visitors to our Web sites, and members participating in our Loyalty Programs,” and promised the use of strong encryption and firewalls.

While Wyndham plans to fight the FTC’s suit, a highly-publicized claim like this puts a hotel firm at a competitive disadvantage. If a hotel chain were known to have faulty locks or in-room safes, guests would think twice before making a reservation. A hotel chain that cannot safeguard the financial and personal information of guests is just as vulnerable.

[Note: Wyndham lost the appeal by decision in August 2015. See What every hotel owner (and operator) needs to know about “data security” after the Wyndham case.]

Beyond Guest Information

While the security of guest information is a key concern, and its breach garners adverse and unwanted publicity, hotel owners and operators should be aware that there is other, valuable information that needs protection. The hospitality
industry is a highly competitive environment, and hotel owners and operators need to take steps to protect their own business information and trade secrets. This information can include pricing strategies and revenue management policies; marketing plans; menus and other food and beverage operations; and perhaps most sensitive of all, employee information. The inadvertent disclosure of this information can cause irreparable harm to a hotel or operator, and steps need to be taken to safeguard competitive and confidential matters.

Another area of potential liability, often overlooked by hotel operators, is the impact of social media. Postings on Facebook, Twitter, Tripadvisor and other social media sites are often treated as less serious than “formal” communications. However, hotels can be held responsible for postings, both those that a firm makes intentionally – for example, in response to a customer review – and those made without clear authorization, like postings by a hotel employee.

What do I do now?

Securing guest and corporate information is a key task, and the steps necessary to implement a secure environment are unique to each organization. However, there are some general considerations that all firms should be aware of that are essential to securing information:

- Hotels operators should inventory potentially sensitive information and document on which computers, servers and laptops it’s stored.
- Operators and owners should keep sensitive information on the fewest number of computers or servers, and be sure to segregate it — the fewer copies of data you have, the easier it is to protect.
- Utilize encryption for storing, and secure connections for receiving or transmitting, credit card information and other sensitive data.
- One of the key claims in the FTC’s case against Wyndham was that Wyndham claimed to have effective privacy measures; in response, firms should design, institute and follow an effective privacy policy, including policies for using social media, and should be careful not to overstate the effectiveness of their measures. Remember – no system is completely safe.
- When implementing a wireless system, use a good firewall and a secure wireless connection.
- For internal communications and information, protect sensitive data with strong passwords and change passwords on a regular basis.
- Since much, if not most, of computer systems and services are handled by vendors, check their security practices.

Most of all, hotel companies need to make a commitment to secure the sensitive information of their companies and their guests, and to seek out informed consultants and advisors. Information security is a relatively new and rapidly changing area, and requires specialized knowledge; the investment today can protect a hotel from being front page news – for the wrong reasons – later.

Here are some of the ways JMBM helps clients with data security matters

The JMBM Global Hospitality Group® and the JMBM Cybersecurity & Privacy Group work with clients to establish and enforce data security policies, and assists clients when there are breaches. We have helped a variety of clients, including hospitality companies, in developing compliance programs, addressing data breach issues, and negotiating contracts with
vendors and providers.

Here are some of the ways we help clients with data security matters:

- Respond to data breaches, including selecting appropriate technology and forensics experts
- Develop and implement data breach response plans and procedures, and related privacy, information security and data retention policies and procedures
- Address statutory and regulatory issues
- Develop effective solutions for protecting and managing information assets and complying with legal requirements, using an approach that will contain costs and maintain operational efficiency
- Advise clients on international privacy laws and rules on their businesses, including the U.S.–E.U. Safe Harbor Program
- Address legal challenges posed by social media and mobile applications
- Negotiate agreements for technologies and services to implement information management systems
- Conduct internal investigations, particularly those involving sensitive electronically stored information
- Assist companies in developing appropriate governance tools to the board of directors and executive management levels to address cyber risk

Click here for more information, including specific examples of projects undertaken for representative clients.

Other information about cybersecurity issues

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

- What every hotel owner (and operator) needs to know about “data security” after the Wyndham case
- What the Target data security breaches mean for hoteliers
- Cyber Security Alert: How to protect your proprietary information from employees
- Hotel Lawyer Privacy Alert: Do your hotel mobile apps comply with new interpretations of online privacy rules?
- Hotel Liability for Guest Information — What you need to know and how to avoid liability.
- Losing the expectation of privacy bit by bit, byte by byte.
- Dodd-Frank Act presents Hotels with decisions on credit and debit card charges.
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. Why don’t you give us a call (or send an email) and let us know what you working on. We would like to see if our experience might help you create value or avoid unnecessary pitfalls. Who’s your hotel lawyer?

Our Perspective. We represent hotel owners, developers and investors. We have helped our clients find business and legal solutions for more than $87 billion of hotel transactions, involving more than 3,900 properties all over the world. We bring this experience to any hotel project — big or small. Let’s explore how it might work for you. For more information, please contact Jim Butler at jbutler@jmbm.com or +1 (310) 201-3526.

Jim Butler is a founding partner of JMBM, and Chairman of its Global Hospitality Group® and Chinese Investment Group™. Jim is one of the top hospitality attorneys in the world. GOOGLE “hotel lawyer” and you will see why. Jim and his team are more than “just” great hotel lawyers. They are also hospitality consultants and business advisors. They are deal makers. They can help find the right operator or capital provider. They know who to call and how to reach them.