akerman

Practice Update

Who Is Liable After a Hotel Data Breach: Owners Or Operators?

February 10, 2017

Co- Authored by Ronald S. Kornreich

It is no secret that more and more businesses are victims of cybercrime. The hospitality sector is not immune. Due to the numerous ways in which hotels collect guest information, they are major targets for cybercriminals.

This issue is exacerbated by the expansion and heightened use of technology. Think about the many ways in which hotels gather and store the personal data of their guests and staff, among others.

Properties acquire sensitive information when guests make reservations, at check-in with new technologies, including mobile check-in and key cards, hotel reward programs, online travel agencies and other third-party marketing partners also collect sensitive, personal information.

Yet, despite the heightened risk to hotel owners and operators of a cybersecurity breach, many hotel management agreements are silent or ambiguous on how to prepare for and respond to a data breach and allocate the responsibility and liability for such a breach between the owner and the operator. Rather than include specific provisions, many management agreements rely on generalized provisions not tailored to the realities and intricacies of data breaches.

Related People

Ronald S. Kornreich

Related Work

Data Privacy and Security
Hospitality
Hospitality Operational Matters
Hospitality Regulatory Compliance

For instance, a management agreement may provide that the owner will indemnify the operator for liabilities associated with the ownership and operation of the property, except for circumstances in which the operator has acted with gross negligence, willful misconduct, bad faith or, in some cases, breach of the management agreement. A management agreement may also impose upon the operator an obligation to comply with, or use some degree of effort to comply with, applicable law.

But absent specific provisions dealing with the treatment of hotel guest personal data and information, these types of generalized provisions can create uncertainty between the owner and operator regarding the response to, and responsibility for, a data breach.

From the operator's perspective, a data breach is no different than a "slip and fall" or employee theft case that is beyond his or her control. Thus, in the operator's view, absent those circumstances in which the operator has acted with gross negligence, willful misconduct or bad faith, liabilities from a data breach should be the owner's responsibility.

Moreover, it is not always the case a data breach will give rise to a violation of law by the operator, as there will likely be an intervening, sometimes criminal, act by a third party.

From the owner's perspective, there are circumstances beyond gross negligence, willful misconduct, bad faith or breach in which the operator should bear the liabilities associated with a data breach.

Many operators take the position that guest data is proprietary to the operator and is not to be shared with the owner, and many state breach notification laws impose reporting and notice obligations on the data owner. In the owner's view, liabilities associated with brand or system-wide breaches (those that are

not specific to any one hotel) are inherently different and fall under the responsibility of the brand/operator.

So what steps should hotel owners and operators take in light of cybersecurity risks?

- Review their hotel management agreements to understand who is responsible for cybersecurity breaches or, if responsibility is not allocated clearly, to understand the risks associated with that ambiguity.
- Consider including provisions in their agreements regarding owner and operator cooperation and specify data management procedures and response plans, including compliance measures and audit procedures with respect to the handling of personal data and information.
- Identify and evaluate the cost and benefits of cybersecurity insurance. Commercial general liability insurance policies often exclude cyber risks.
- Ensure both owner and operator are insureds under any cybersecurity policy. Keep in mind that an operator's insurance may not cover the owner, and vice versa.
- Consider the scope of cybersecurity coverage. Proper insurance should include both first-party coverage (direct losses including fraud monitoring, breach notification and legal costs) and third-party coverage (including damages to affected parties).
- Test agreed upon procedures and response plans to ensure their effectiveness.
- Identify external vendors who will assist with crisis management, forensic investigations and breach notifications in the unfortunate event a breach occurs. Negotiate in advance of a breach appropriate vendor retainer agreements.

While, of course, the threat of a data breach cannot be eliminated completely, understanding the risks and maintaining appropriate levels of insurance coverage are essential to mitigating the potential harm that may ensue from a cyber-attack.

This updated originally published in *Hospitality Technology* on February 10, 2017.
