New York Law Journal
Real Estate Trends
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 35
WEDNESDAY, AUGUST 20, 2014

HOSPITALITY LITIGATION

Protection of Hotel Guest Data And Personal Information



By **Todd E. Soloway**
And **Joshua D. Bernstein**
And **Jared Newman**

Think back to your most recent stay at a hotel. Did you leave anything behind? If you paid for your stay with a credit card, then you likely left your personal financial information at the front desk. If you indulged in a spa treatment, then you might have left your medical information as well. If you dined, booked another stay, or enrolled in a hotel loyalty program, then you also left valuable information about your lifestyle and behavior. Disclosure of such personal information has become commonplace in the hospitality industry and the world at large, and hotel guests reasonably assume that hotels are safeguarding this sensitive, personal information. However, ever-growing numbers of sophisticated computer hackers and cyber-criminals appear to be focusing their attention on stealing the personal information of hotel guests despite the often state-of-the-art data security systems implemented by the hospitality industry to protect it.

Given the increasing sophistication of computer hackers and their ability to infiltrate even the best designed data security systems, a question often arises following the theft of such personal information as to the extent of a hotel company's liability to guests whose personal information was stolen. While virtually every state, including New York,[1] has enacted laws that require a company to disclose a data breach to its customers once a security breach has occurred, there is a dearth of law or statutes regulating what measures a company, including hotel managers, must implement to protect its guests' sensitive and personal information in the first instance.

Especially in the case of hotel managers and owners, which, as explained below, are in a unique position of being obligated to protect guests and their property from harm (i.e., common law innskeeper liability), courts are increasingly forced to grapple with what duty, if any, a hotel manager or owner actually owes to its guests under these circumstances. And, given that it has proven difficult for an individual person to prove and thus recover damages once a data breach has occurred, to what standard of liability should a hotel manager/owner be held in the event of a data breach? This article examines these issues.

Duty to Protect

When a guest checks in at a hotel, or runs his or her credit card for a spa treatment, the hotel manager or owner does not sign a contract to protect that individual's financial and personal information from cyber-criminals. Thus, if a hotel manager or owner is to bear any liability for the loss or theft of a guest's personal information, that liability will derive in tort or from statute rather than from a breach of contract. But does a hotel owner or manager have a tort-based or statutorily imposed duty to protect its guests' personal and financial information?

The Federal Trade Commission (FTC) currently serves as the primary administrative body for enforcing electronic data security,[2] and a hotel owner/manager's statutory duty to protect a guest's information derives, if at all, from the Federal Trade Commission Act (FTC Act), which protects consumers by prohibiting "unfair" acts or practices in commerce.[3] Section 5 of the FTC Act defines an "unfair act or practice" as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[4] The relationship between a hotel owner/manager and its guest with respect to the protection of personal and financial information appears to fit squarely within the protections of the FTC Act as (i) a hotel guest has no way of implementing measures or taking action to protect their information once they have transmitted that information to the owner/manager; (ii) there is no countervailing benefit to other consumers, other than criminals, or to competition that is being suppressed or harmed by implementing data security measures; and (iii) a cyber-criminal stealing a guest's credit card and other financial information has the potential to cause substantial injury to the hotel guest.

That a hotel owner/manager has a duty to provide adequate data security measures to protect the information of its guests was established in *Federal Trade Commission v. Wyndham*, in which the United States District Court of New Jersey confirmed the FTC's authority to allege a hotel manager acted "unfairly" by failing to provide an adequate data security system.[5] In *Wyndham*, the FTC sued Wyndham Worldwide Corporation following a data security breach in which hackers obtained access, via the hotel's computer network, to guests' credit and debit card account numbers, expiration dates and security codes.[6] The breach resulted in the compromise of more than 619,000 consumer account numbers and the loss of more than $10.6 million to those guests.[7] The FTC alleged that Wyndham had maintained "unreasonable data-security practices," "fail[ed] to address its data-security flaws,"[8] and had engaged in "a number of practices that, taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft."[9] Wyndham moved to dismiss the FTC's "unfairness" claim, arguing, among other things, that the FTC's allegations were pleaded insufficiently to support a claim under Section 5 of the FTC Act.[10] The court rejected Wyndham's argument, holding that the FTC had sufficiently pleaded an "unfairness" claim under the FTC Act,[11] reasoning that the agency's allegations of fraudulent charges affecting numerous hotel guests satisfied the "substantial injury" requirement of Section 5.[12] The court further declined to find that, "as a matter of law, any financial injury from payment card theft data is reasonably avoidable" by consumers.[13]

The court, despite making no determination regarding liability, held that hotel managers/owners—at the very least—owe guests a duty not to engage in unfair data security practices. Notwithstanding the decision, the duty that a

TODD E. SOLOWAY *and* JOSHUA D. BERNSTEIN *are partners at Pryor Cashman.* JARED NEWMAN, *an associate at the firm, and* DANIELLE TEPPER, *a summer associate at the firm, assisted in the preparation of this article.*

hotel owner/manager owes to its guests is vague, undefined and fails to guide the hotel in any reasonable manner as to what it is required to do. Yet, *Wyndham* held, the hotel owner/manager can be found to have breached that duty.

Breach of Duty

As detailed above, the present amorphous duty and standard of care leaves the hospitality industry guessing as to the sufficiency of the security systems they have in place or might desire to implement in the future. Thus, the next issue that must be determined is the standard of liability that should be imposed on a hotel owner or manager for a data breach. In other words, should a hotel owner/manager that has suffered a data breach be held to a negligence standard or should hotels, given their unique access to deeply personal information, be held to a higher standard such as a strict liability standard for data theft?

Negligence Standard. The standard of care set forth in the FTC Act most closely resembles a negligence standard. This is because, while the act prohibits "unfair acts or practices," it provides no specific guidance regarding the acts which constitute "unfair acts or practices" in the data security context. Wyndham argued that the FTC should be required to formally promulgate regulations explaining "what data-security practices the Commission believes Section 5 to forbid or require" before it could bring its unfairness claim.[14] However, the court declined to require the FTC to promulgate specific guidelines, and instead applied a negligence standard based on the FTC's ability to exercise discretion in making Section 5 enforcement decisions, analogizing that other agencies in similar circumstances have brought enforcement actions without having in place particularized prohibitions, and also specifically acknowledging that such a standard, ultimately being based on reasonableness, is appropriate given the "rapidly-evolving nature of data security."[15]

Although the court rejected Wyndham's argument, the argument has real merit for the very same reasons the court applied a negligence standard—i.e., based on the realities and "rapidly-evolving nature of data security." What the Wyndham court did not fully appreciate or address is that the absence of clearly-defined guidelines hurts both hotel owners/managers and guests, leaving all parties wondering, albeit for different reasons, whether the owner/manger has satisfied its duty and has done enough to protect the guests' financial and personal information, or whether it has breached that duty and is subject to liability in the event of a data breach. With virtually every hotel company already having in place some form of security system, neither the company nor the guests benefit from a vague standard requiring only that a hotel company be better than negligent.

The Rule of Infra Hospitium. At the other end of the spectrum lies a standard of strict liability—a rigid standard with which the hotel industry is not unfamiliar. Under the historical common law rule of infra hospitium, an innkeeper "was an insurer of goods delivered into his or her custody by a guest," and therefore was absolutely liable for a guest's loss of property despite "not having any culpability for the property's theft or destruction."[16] This common law rule has largely been superseded by state statutes limiting a hotel's liability for loss or theft of tangible property because the dangers it was meant to protect against are no longer present in this day in age, which was "when travel was perilous, highway robbers abounded, and the only safe sanctuary at night usually was an inn."[17]

> Given the increasing sophistication of computer hackers and their ability to infiltrate even the best designed data security systems, the question often arises following the theft of personal information as to the extent of a hotel company's liability to guests whose personal information was stolen.

Although highway robbers no longer abound, the threat posed by computer hackers and cyber-criminals on the information super-highway is real and serious, and thus, a standard of strict liability seems at least conceptually appropriate to govern liability to guests in the event of a data breach. But, for a similar reason that a negligence standard does not consider the realities of data security, the harsh result under a strict liability standard imposes too great of a burden on the hotel owner/manager by holding it liable for any and all data security breaches regardless of the precautions taken, especially in the face of a cyber-criminal community that is constantly evolving and developing new, cutting-edge ways to infiltrate the hotel's computer systems. While certain global hotel management companies may have the financial resources to keep pace, it is economically not viable to uniformly impose such a burden across the industry.

Negligence Per Se. Although it has yet to be addressed by the courts, the solution may be the negligence per se standard. Under a negligence per se standard, whereby negligence is established as a matter of law, an appropriate balance can be drawn. This is because a party can obtain relief for the unexcused breach of a statutory duty if (i) that party is a member of a class intended to be protected by a statute; and (ii) the violation of the statutory duty proximately caused the party's injury.[18]

For example, under General Business Law §200, hotels in New York (a) must install and maintain a safety chain latch on each unit door; and (b) may limit liability for loss of property by providing a safe or safety deposit boxes.[19] If the hotel owner/manager fails to implement these protective measures (which would be the proximate cause of the injury), the hotel owner/manager will be liable to the guest (a member of a clearly defined class intended to be protected by the statute). This statutory regime succeeds in providing guests with adequate security while also providing hotels with fair notice as to what they are required to do and what is expected of them.

The data security landscape of the hotel industry would benefit from a similar—though more detailed—statute or FTC regulation specifying a hotel owner/manager's duty and enumerating the data security measures that are required to be implemented in order to satisfy that duty. A statute structured under this framework protects the hotel guests—since it is undeniable that hotel guests are an easily identifiable class of people who are turning over their financial and personal information to the hotel—while also setting forth clear and enumerated guidelines that hotel owners and managers must follow. Under such a structure, the hospitality industry will know if its security measures are compliant and sufficient to avoid liability.

Conclusion

As is evident from the above discussion, the law governing liability for the theft of customer data in general, and the theft of hotel guest data in particular, is developing as we speak. As a result, the current state of the law leaves those in the hospitality industry with significant uncertainty as to how to proactively protect themselves from liability for a data breach. Even where a hotel company implements a state-of-the-art data protection plan, it may nonetheless face liability if courts apply a traditional infra hospitium rule to the theft of hospitality guest data. This uncertainty is likely to continue until the Legislature or the FTC takes action to clearly define the responsibilities and liabilities for the hotel industry.

1. New York General Business Law §899-aa; New York State Technology Law §208
2. Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583, 600 (2014).
3. See 15 U.S.C. §45(a).
4. See 15 U.S.C. §45(n).
5. *FTC v. Wyndham Worldwide Corp.*, 2014 U.S. Dist. Lexis 47622 (D.N.J. Apr. 7, 2014).
6. Id. at *5-6.
7. Id. at *6-7.
8. *Wyndham Worldwide*, 2014 U.S. Dist. LEXIS at *45.
9. Id. at *5.
10. See id. at *3.
11. Id. at *45-46.
12. Id. at *46.
13. Id. at *55.
14. Id. at *27.
15. Id. at *38-41.
16. See *Goncalves v. Regent Intern. Hotels*, 58 N.Y.2d 206, 214-15 (1983).
17. Id. at 214.
18. See *Dance v. Southampton*, 95 A.D.2d 442, 445-46 (2d Dep't 1983).
19. NY GBL §200.