New York Law Journal
Real Estate Trends
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 89
WEDNESDAY, MAY 10, 2017

Hospitality Litigation

Assessing Risk to Hotels In the Age of Data Breaches

By **Todd E. Soloway** And **Bryan T. Mohler**

With each passing day, the public is inundated with more reports of data breaches affecting companies of all shapes, sizes and types. The hospitality industry has not been spared from exposure to such breaches, and in fact several of the most widely publicized incidents involve some of the largest hotel brands in the world. Just weeks ago, InterContinental Hotels Group (IHG) announced it had suffered a data breach at multiple IHG-branded franchise hotel locations in the United States and Puerto Rico in late 2016. This comes on the heels of IHG's disclosure in February of a separate malware attack exposing customer data at 12 U.S. IHG-managed hotels. IHG is not alone, as Wyndham Worldwide, Hard Rock Hotels, Omni Hotels & Resorts and Hilton Hotels, among others, have all been publicly cited as victims of cyber-attacks and resulting data breaches.

While much has been reported on these incidents, less is understood about what liability may flow from a hotel data breach. Among the questions are which party or parties may bring actions after a data breach, against whom, and for what damages. Separately, as among the impacted hotel's operator and owner, and its general liability insurer, which party or parties are ultimately liable for any losses caused by a data breach. This article explores these issues.

Potential Complainants?

Consumers. When a hotel guest's financial or personal information is compromised as a result of a data breach at a hotel, it stands to reason that the guest could bring suit against the hotel operator and/or owner. The answer is not as clear as one would think, and ultimately may depend upon the type of information that is compromised. In a recent decision by the Southern District of California in *Dugas v. Starwood Hotels & Resorts Worldwide*, No. 16-cv-00014, 2016 WL 6523428 (S.D. Cal. Nov. 3, 2016), a key issue was whether a consumer can sufficiently allege that she suffered an "injury in fact" such that she has standing to sue under Article III of the U.S. Constitution. Id. at *2-3.

The court distinguished between the theft of social security information or usernames and passwords, on the one hand, and theft of names, addresses, or credit card numbers, on the other hand. It noted that the former may constitute "real and immediate harm" to consumers so as to confer Article III standing because cyber-criminals can use such information to commit identity theft.

By contrast, the court found that billing information and credit card numbers—for since-canceled credit cards—are insufficient "for a third party to open up a new account in plaintiff's name or to gain access to personal accounts likely to have the information needed to open such an account (e.g., a social security number)." Id. at *5.

In another class action, however, this time against Kimpton Hotel & Restaurant Group, a federal court held just weeks ago that "[t]he theft of [a consumer's] payment card data and the time and effort he has expended to monitor his credit are sufficient to demonstrate injury for standing purposes." *Walters v. Kimpton Hotel & Restaurant Group*, No. 16-cv-05387, 2017 WL 1398660, at *1 (N.D. Cal. April 13, 2017). This same rationale led the court to find that the plaintiff had sufficiently alleged "actual damages" for purposes of his claims for breach of implied contract, negligence, and certain violations of California's Unfair Competition Law. Id. at *2. Similar causes of action had been alleged in yet another data breach litigation against Trump International Hotels Management, although that

TODD SOLOWAY *and* BRYAN MOHLER *are partners at Pryor Cashman.* DANIELLE TEPPER, *an associate at the firm, assisted in the preparation of this article.*

action ultimately was voluntarily dismissed. *Driscoll v. Trump Int'l Hotels Mgmt.*, No. 15-cv-01089 (S.D. Ill. Oct. 2, 2015). The plaintiff in that case sued for, among other things, violations of state consumer protection laws. Id.

While the case law in this area is still developing, it appears that courts will rigorously scrutinize consumer suits with a particular focus on whether and how a consumer alleges to have been harmed by a data breach.

Regulators. Just as consumers may look to state consumer protection laws for redress following a data breach, the Federal Trade Commission (FTC) has the authority to regulate cybersecurity under the "unfairness" prong of 15 U.S.C. §45(a). See *F.T.C. v. Wyndham*, 799 F.3d 236 (3d Cir. 2015). In *Wyndham*, the FTC sued Wyndham Worldwide in federal court, alleging that its conduct of allegedly failing to maintain reasonable and appropriate data security for consumers' personal information constituted an unfair practice and that its privacy policy was deceptive. See id. at 240. The district court denied Wyndham's motion to dismiss, and the U.S. Court of Appeals for the Third Circuit affirmed, holding that Wyndham's alleged failure to maintain reasonable and appropriate data security, if proven, could constitute an unfair method of competition in commerce under §45(a). Under 15 U.S.C. §53(b), a court may grant injunctive relief to halt and redress violations of any provision of law enforced by the FTC.

Credit Card Companies. Many credit card service agreements contain provisions entitling the credit card issuer to sanction merchants when a data breach occurs. As revealed in a recent lawsuit filed against Rosen Millennium Technology Group (Rosen), a subsidiary of Rosen Hotels & Resorts, arising out of a data breach that affected customers of Rosen's various hotels, such penalty provisions can impose substantial additional costs for hotels in the wake of a data breach. In *St. Paul Fire & Marine Ins. v. Rosen Millennium,* No. 17-cv-00540 (M.D. Fla. March 27, 2017), an insurance company sought a declaratory judgment declaring that Rosen's insurance policy did not provide coverage for Rosen's claims arising from the alleged data breach. In the insurance company's complaint, the company alleged that, "[a]s a result of the alleged attack and the findings of the investigation, and in accordance with their respective card services agreements, Visa, MasterCard, and American Express allegedly imposed substantial fines on Rosen." Id. According to the complaint, those fines were in the amounts of $1,005,139.71for MasterCard; $128,830 for American Express; and over $1 million for Visa. Id.

> As among the hotel's operator and owner, and its insurer, which party or parties are ultimately liable for any losses caused by a data breach?

Who Is Liable?

It is generally the case that hotel operators, rather than hotel owners, are the entities that collect and store guests' financial and personal information. But that does not mean that hotel owners will escape liability in the event of a data breach, as most hotel management agreements contain language obligating the owner to indemnify the operator, depending upon the vintage of the contract. While this language generally was envisioned to cover slip-and-fall/third-party type liability, and not liability arising out of a data breach, hotel operators are likely to take aggressive positions that such language places all risk on the hotel owner. Thus, owners would benefit from considering the implications of a potential data breach before it strikes.

Importantly, as the Rosen case demonstrates, relying on a general liability insurance policy is risky. A hotel's general liability insurer is unlikely to cover damages arising from a data breach, and rather will take the position that such policies cover only bodily injury and property damage. "[C]ourts have consistently stated that data is not property and is considered intangible." Dena L. Magyar, "Understanding the Impact of a Data Breach on your Hotel or Resort," Wells Fargo Insurance (January 2014). As a result, purchasing cyber liability insurance may be the most effective way for hotel owners to protect themselves in the event of an unexpected data breach.

Conclusion

The hotel industry and the consuming public alike would prefer to avoid data breaches entirely. But in an age of rapid technological advancement—including for cyber-criminals—hotel owners should not underestimate the value of being prepared. This means both knowing to whom a hotel might be liable in the event of a breach and understanding which entity or entities will ultimately be responsible for footing the bill. If your general liability insurance policy will not cover such costs, you should be aware of that and consider investing in a policy that will. Hotel owners negotiating a hotel management agreement also would be wise to pay careful attention to any indemnification language, and make every effort to protect themselves in situations where a data breach occurs through no fault of their own.