

## **HOTEL LAW: CYBERSECURITY AND RESORT FEES**

**April 25, 2017**

By Thomas A. Dickerson<sup>1</sup>

Two of the more annoying and unexpected occurrences when vacationing at a lovely luxury hotel is to have your personal and financial data hacked and/or to be forced to pay an undisclosed resort fee as you are checking out. Both occurrences are increasing in frequency in the hotel industry and have been the subject of lawsuits and investigations by the Federal Trade Commission (FTC). In addition, hotel call centers may record customer phone calls without authorization<sup>i</sup>.

### **Wyndham Cybersecurity Breach**

In *Federal Trade Commission v. Wyndham Worldwide Corporation*<sup>ii</sup> [Wyndham] hackers were able to obtain the personal and financial information of 619,000 Wyndham hotel guests leading to this

---

<sup>1</sup> Thomas A. Dickerson is of counsel to Herzfeld & Rubin and the author of *Travel Law*, Law Journal Press (2017). Mr. Dickerson is a former Associate Justice of the Appellate Division, Second Department of the New York State Supreme Court.

enforcement action alleging "unfairness" because of several data security insufficiencies and "deception" by overstating Wyndham's privacy policy on its websites. On three occasions in 2008 and 2009 hackers successfully accessed Wyndham computer systems resulting in over "\$10.6 million dollars in fraudulent charges". In the first cyber attack hackers broke into the local network of a hotel in Phoenix, Arizona which was connected to Wyndham's network and the Internet. "They then used the brute-force method...to access an administrative account...

Obtained encrypted information for over 500,000 accounts which they sent to a domain in Russia". The second cyber attack accessed the same administrative account resulting in access to another 50,000 guest accounts from property management systems of 39 hotels. Two months later Wyndham discovered the existence "'memory-scraping malware' used in the previous attack on more than thirty hotels' computer systems". In the third cyber attack hackers again accessed an administrative account obtaining data on another 69,000 guests.

### **Specific Cybersecurity Failures**

In affirming the District Court the Third Circuit Court of Appeals found that the FTC had the authority to regulate cybersecurity under the unfairness prong of Section 45(a) of the FTC Act and that Wyndham had fair notice that its cybersecurity practices could fall

short of that provision. The Court agreed with the FTC's finding of specific security failures to include

(1) allowing "Wyndham-branded hotels to store payment card information in clear readable text", (2) allowing the use of "easily guessed passwords to access property management systems", (3) failure to use "'readily available security measures such as firewalls", (4) failure to "ensure that the hotels implemented 'adequate' information security policies and procedures", (5) failure to "'adequately restrict' the access of third-party vendors to its network", (6) failure to "'conduct security investigations'", and (7) failure to "follow 'proper incident response procedures'".

### **Starwood Cybersecurity Breach**

In *Dugas v. Starwood Hotels and Resorts Worldwide, Inc.*<sup>iii</sup> the Court noted that "This case arises from a series of attacks by criminal hackers upon the United States hospitality industry". Alleging, *inter alia*, the violation of California's Customer Records Act (CRA) and Unfair Competition Law (UCL), invasion of privacy and negligence, the plaintiff asserted that "customer systems of Starwood Hotels and Resorts Worldwide, Inc. (Starwood) had malicious software installed on them and they have been compromised since 'at least November 2014'... According to Plaintiff, although Starwood 'discovered the first data breach on or around April 13, 2015', they

failed to notify customers or regulators of the data breach 'until November 20, 2015 via [] internet press release. Within said press release, Starwood revealed 'that hackers had breached its database containing sensitive records including names, credit card numbers, security codes and expiration dates'".

### **Claim Stated**

In denying a motion to dismiss, in part, the Court found that plaintiff's allegations that he lost time and money in the process of mitigating financial losses caused by the Starwood breach were sufficient to state an injury in fact. The Court also found "a legal duty and a corresponding breach as to inadequate security measures (under the CRA citing *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*<sup>iv</sup>).

### **French Lick Data Breach**

In *Alonso and Hardt v. Blue Sky Resorts, LLC*<sup>v</sup> in which plaintiffs, hotel guests, respectively, at "Blue Sky's West Baden Springs Hotel" and "Blue Sky's French Lick Spring Hotel" sought to represent a class of hotel guests seeking damages arising from a data breach committed by hackers who had installed a malware program on one of the servers on French Lick Resort's point of sale system.

This malware allowed the hackers to periodically obtain certain credit information from some, but not all, of the resort's customers who had used their credit cards at the resort—specifically the names, credit card numbers and card expiration dates were stolen. In dismissing the plaintiffs claims the Court noted that Defendants asserted that Plaintiffs did not suffer any damages because they failed to allege that their “credit card accounts ever had any fraudulent charges made on them”. The Court determined that Plaintiffs lacked Article III standing because they had not alleged nor suffered a concrete, particularized injury. “Additionally, they cannot demonstrate that any future injury they fear is certainly impending”.

### **Resort Fees: The FTC Report**

Perhaps, the most annoying problem for hotel guests is the imposition of undisclosed resort fees<sup>vi</sup>. On January 5, 2017, the Federal Trade Commission (FTC) issued a Report, *Economic Analysis Of Hotel Resort Fees*<sup>vii</sup>. In November 2012, the FTC warned 22 hotels that resort fees were not adequately disclosed on their hotel reservation websites, and that such practices may violate the law by misrepresenting the price consumers expected to pay for their hotel rooms. In response to these warning letters, many hotels modified their resort fee disclosures. “Despite improvements in

resort fee disclosures since 2012, complaints about the fees persist. Consumers and advocacy groups, including Travelers' United, argue that not including resort fees in the room rate makes it more difficult for consumers to comparison shop".

### **Consumers Harmed**

The FTC's analysis found that separating mandatory resort fees from posted rates without first disclosing the total price is likely to harm consumers by increasing the search costs and cognitive costs of finding and choosing hotel accommodations. "In this situation, a consumer's choice is either to incur higher total search and cognitive costs or to make an incomplete, less informed decision that may result in a more costly room, or both."

### **The Luca Case**

In Luca v. Wyndham Worldwide Corp.<sup>viii</sup>, a class action, the plaintiff alleged that he accessed a hotel reservation website and purchased a hotel room that he would not otherwise have purchased "absent Defendants' deception". In the complaint plaintiff identified the cost of the room, the allegedly undisclosed or misrepresented costs and taxes and the "final cost stated on the invoice presented after his hotel stay" which allegedly violated

the New Jersey Consumer Fraud Act (CFA) and the New Jersey Truth-In-Consumer Contract, Warranty and Notice Act (TCCWNA). Some defendants' moved to dismiss the complaint on the grounds, *inter alia*, that the website's disclosures were adequate and, in any event, the plaintiffs failed to plead an ascertainable loss. In denying the motion the Court found that "given Plaintiff's substantially unmet contention that the total invoiced amount was never disclosed on the website" sufficiently asserted a quantifiable loss under the CFA. And further, "the present Plaintiff's allegedly defeated expectations relate to the price that he was led to believe that he would pay for the product versus the price ultimately charged".

## **Conclusion**

It is clear that the criminal hacking of hotel computers and the theft of personal financial data as well as the imposition of undisclosed or inadequately disclosed resort fees are problems which are likely to continue. Consumer may be careful in protecting their personal information and resisting, if possible, the imposition of undisclosed resort fees.

ENDNOTES

- 
- i. See *McCabe, Simpson & Sarabia v. Six Continents Hotels, Inc.*, Case No. 12-cv-04818-NC (N.D. Cal.) (a class action settlement notice stated “A proposed \$11,700,000 class action settlement has been reached (in the McCabe class action which) claims that (defendants) recorded and monitored telephone calls of persons calling toll-free reservations and customer-service lines... without telling callers that the call may be recorded or monitored”). See Dickerson, *Travel Law: Unauthorized recording of phone calls to hotel call centers*, [www.eturbonews.com](http://www.eturbonews.com) (11/19/2015).
- ii. *Federal Trade Commission v. Wyndham Worldwide Corporation*, 2015 WL 2812049 (D.N.J. 2014), *aff’d* \_\_ F. 3d \_\_ (3<sup>rd</sup> Cir. 2015).
- iii. *Dugas v. Starwood Hotels and Resorts Worldwide, Inc.*, 2016 WL 6523428 (S.D. Cal. 2016).
- iv. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014)
- v. *Alonso and Hardt v. Blue Sky Resorts, LLC*, 2016 WL 1535890 (S.D. Ind. 2016).
- vi. See Kieler, *Hotels Harm Consumers By Not Including ‘Resort Fees’ In Room Rates*, <https://consumerist.com> (1/5/2017) (“Staying in a hotel comes at a price—there’s the room rate, service charges, taxes and hotels are increasingly taking on ‘resort fees’ to cover amenities like internet access, parking, gym, spa and pool—even if you never use them. These fees, which can significantly increase the total cost of a room, are almost never included in the advertised price and are often minimized or omitted until it comes time to actually book your stay”).
- vii. *Economic Analysis Of Hotel Resort Fees* at [www.ftc.gov/reports/economic-analysis-hotel-resort-fees](http://www.ftc.gov/reports/economic-analysis-hotel-resort-fees) (“This paper examines the likely costs and benefits of disclosing resort fees separately from the room rate by reviewing the economics and consumer behavior literatures on drip pricing and partitioned pricing, two pricing practices used by online travel agents and hotels to disclose resort fees to consumers. Partitioned pricing entails dividing the price into multiple components without disclosing the total. Drip pricing is the practice of advertising only part of a product’s price upfront and revealing additional charges later as consumers go through the buying process”).
- viii. *Luca v. Wyndham Worldwide Corp.*, 2017 U.S. Dist. LEXIS 21433 (W.D. Pa. 2017)..