TRAVEL LAW: THE WYNDHAM DATA BREACH CASE: LESSONS TO BE LEARNED IN CYBERSECURITY

REVISION #2

September 11, 2015

One year ago we discussed a case involving hackers who had obtained personal information on 619,000 hotel guests of Wyndham Worldwide Corporation [Wyndham][see *Are Tourists Safe from Hackers and Negligent Suppliers?*, www.eturbonews.com (9/24/2014)]. That case, *Federal Trade Commission v. Wyndham Worldwide Corporation*, 2014 WL 2812049 (D.N.J. 2014) resulted in a decision finding that the FTC had sufficiently pled claims against Wyndham under the Federal Trade Commission Act for "unfairness" by specifically setting forth data security insufficiencies and "deception" by overstating its privacy policy on its website. Recently, the U.S. Court of Appeals for the Third Circuit affirmed the District Court's decision.

Travel Law Update

Money Losing Flights & Golden Parachutes

In Zernike & Mouawad, *United C.E.O. Is Out Amid Inquiry at Port Authority*, www.nytimes.com (9/9/2015) it was noted that "The chief executive and two senior officials of United Airlines resigned on Tuesday amid a federal investigation into whether the airline had traded favors with the Chairman of the Port Authority of New York and New Jersey. The United States attorney for New Jersey has been investigating whether United, the nation's third-largest airline, agreed to reinstate money-losing flights to the airport nearest the weekend home of the authority's chairman, David Samson, in return for improvements the airline wanted at Newark Liberty International Airport, where it is the biggest carrier...United filed a report with the (SEC) on Tuesday indicating that Mr. Smisek would receive nearly $4.9 million in a separation payment, and 60,000 shares of stock, valued at over $3 million".

And in Editorial Board, *United Airlines and the Port Authority*, www.nytimes.com (9/9/2015) it was noted "That United Airlines would try to curry favor with Port Authority officials should come as no surprise. It is the biggest airline at Newark, controlling two-thirds of all flights at the airport...Had there been more competition at the airport, authority officials and Newark's top tenant might not have been able to trade favors so

easily. The authority's shady operations might have remained secret but for the four days in 2013 when Mr. Christie's appointees shut down traffic lanes on the George Washington Bridge as punishment for a political rival. The episode promoted federal investigators to take a harder look at the authority's management, including how the agency's $8.2 billion budget was used by governors of New Jersey and New York...The only permanent solution is to change the laws. Legislators in both states must pass exactly the same set of strong reforms to ensure transparency, provide public notice about coming decisions and create protections for whistle-blowers".

Crash Victims' Families May Sue In U.S.

In *Crash victims' families to sue German airline in US court*, www.eturbonews.com (8/10/2015) it was noted that "The families of passengers killed in the Germanwings crash will take legal action against Lufthansa in the United States after rejecting the carrier's compensation offer as inadequate, the Bild am Sontag newspaper reported, citing the families' lawyer. Germanwings, a unit of Lufthansa, in June offered E25,000 per victim and the pain and suffering caused by the March 24 crash that killed all 150 onboard. The E25,000 offer is on top of E50,000 per passenger already paid as immediate financial

assistance to relatives...Germanwings yesterday declined to comment on the report but said compensation would be 'at least E100,000 per passenger and, depending on families' circumstances, reach a high six-digit amount that could rise up to a million euro".

Terror In Tajikistan

In *Terrorist attacks in Tajikistan: Airport attacked twice, UK issues travel advisory*, www.eturbonews.com (9/4/2015) it was noted that "Dushanbe, Tajikistan...was rocked by terrorist attacks on security personnel as the capital of Tajikistan witnessed two separate incidents in which around 11 policemen and security personnel were killed".

Screeners Need To Screened

In *TSA screener at JFK caught stealing $7K diamond watch*, www.eturbonews.con (9/6/2015) it was noted that "A (TSA) screener has been charged with stealing a passenger's $7,000 diamond watch from a plastic bin at Kennedy Airport security checkpoint".

Watch Out For Drones

In *FAA: Pilot reports of unmanned aircraft up dramatically in 2015*, www.eturbonews.com (8/13/2015) it was noted that "Pilot reports of unmanned aircraft have increased dramatically over the past year, from a total of 238 sightings in all of 2014 to more than 650 by August 9 of this year. The FAA wants to send out a clear message that operating drones around airplanes and helicopters is dangerous and illegal. Unauthorized operators may be subject to stiff fines and criminal charges, including possible jail time".

In *Drone World Expo draws commercial users from around the world*, www.eturbonews.com (8/19/2015) it was noted that "More than 600 commercial drone end users representing 17 countries have already registered for Drone World Expo...Conference Program Sessions to be offered include Avoiding the Traffic Jam: A Government and Industry UTM Update, Drones and Privacy: Addressing Public Concern" and other topics.

And in Nicas, *California Gov. Vetoes Drone Restrictions; Win For Amazon, Google*, http://blogs.wsj.com/digits (9/10/2015) it was noted that "California Gov. Jerry Brown vetoed a bill...that would have effectively banned drone flights over private property without permission, a major victory for companies such as Google and Amazon.com that want to use the devices to deliver small packages".

California Uber Driver Is Employee

In Isaac and Singer, *California Says Uber Driver Is Employee Not a Contractor*, www.nytimes.com (6/17/2015) it was noted that "In a ruling that fuels a long-simmering debate over some of Silicon Valley's fastest-growing technology companies and the work they are creating, the California Labor Commissioner's Office said that a driver for the ride-hailing service Uber should be classified as an employee, not an independent contractor...The ruling does not apply beyond Ms. (X) and could be altered if Uber's appeal succeeds. Uber has also prevailed in at least five other states in keeping its definition of drivers as independent contractors...'Defendants hold themselves out as nothing more than a neutral technological platform, designed simply to enable drivers and passengers to transact the business of transportation', the Labor Commissioner's Office wrote about Uber. 'The reality, however, is that defendants are involved in every aspect of the operation'".

Compete With Uber Or Die

In Engquist, *Judge rules on taxi-industry lawsuit: Compete with Uber or die*, Crane's New York Business (9/9/2015) it was noted that "A state judge has slammed the door on a legal

challenge by opponents of Uber, clearing the way for the rideshare giant to tun traditional taxis off the road. In a decision unveiled Wednesday, Queens Supreme Court Justice Allan Weiss ruled that for-hire vehicles could use electronic hails to compete with yellow cabs-something they have been doing well enough to threaten the existence of the iconic 80-year-old industry.

As noted by the Court in *XYZ Two Way Radio Service, Inc. V. The City of New York*, Index No. 5693/15, Decision 9/28/2015, Queens Sup. (J. Weiss) "The is case arises from the introduction of new technologies in the ground transportation industry that are used to dispatch vehicles and to connect passengers with drivers. The use of a smartphone application to obtain a ride has blurred the distinction between a street hail and a pre-arrangement and has disturbed the balance of economic interests within the industry...This case fundamentally concerns an administrative determination to classify and treat passenger communications to companies like Uber as a type of pre-arrangement rather than as a hail".

Uber Background Checks Challenged

In Toutant, *Class Suit Targets Uber's Pre-Employment Background Checks*, New Jersey Law Journal (9/4/2015) it was noted

that "Uber Inc. has been hit with a putative class action in federal court in Newark claiming it violates the Fair Credit Reporting Act (FCRA) by using background records in hiring decisions without allowing applicants to dispute entries in their reports. The case, *Cuccinello v. Uber*, was filed Sept. 2 on behalf of persons who applied for jobs with Uber and were subjects of an adverse employment action based on information from a consumer reporting agency. The suit claims Uber violated FCRA by failing to give each applicant a copy of their report and a summary of their rights under the FCRA before the hiring decision was made".

Missed Criminal Records

In Dougherty, *Uber Missed Criminal Records of Drivers, Prosecutors Assert*, www.nytimes.com (8/19/2015) it was noted that "For more than a year, regulators in various cities have questioned whether Uber...vets its drivers from criminal backgrounds as carefully as traditional taxi companies. Now the district attorneys of San Francisco and Los Angeles have offered perhaps the most concrete evidence to date that people convicted of murder, sex offenses and various property crimes have driven for Uber, despite assurances from the company that it employs 'industry-leading' screening. The district attorneys said

Wednesday that background checks used by Uber failed to uncover the criminal records of 25 drivers in the two cities. The charges were made in a 62-page amended complaint to a civil suit, originally filed in December, that claims Uber has continually misled consumers about the methods it uses to screen drivers... The suit...does not name the criminals but includes some details about the crimes. One driver was convicted of second-degree murder in Los Angeles in 1982 and spent 26 years in prison... He applied to be an Uber driver under a different name from those in his court records...One driver was convicted of felony sexual exploitation of children in Wyoming in 2005, and another of 'felony kidnapping for ransom with a firearm' in 1994. Other drivers were convicted of charges like robbery, assault with a firearm, identity theft and driving under the influence. Several were convicted of more minor charges, like welfare fraud".

Uber Battle In Florida

In Ampel, *Uber Wants Drivers Classified as Independent Contractors*, www.dailybusinessreview.com (8/17/2015) it was noted that "Uber...fought to treat its Florida drivers as 'partners' rather than employees in an appellate hearing Monday...State Department of Economic Opportunity special deputy Jackson Houser heard the appeal of a state decision that Uber drivers should be

considered employees, not independent contractors...Uber is fighting similar battles across the country to hold onto the advantages of classifying workers as independent contractors".

Delayed Flight Compensation Awaiting

In *Airlines owe British flyers millions in delayed flight compensation*, www.eturbonews.com (8/9/2015) it was noted that "London, England-Delayed airline passengers would be missing out on millions of pounds worth of compensation, a consumer investigation has claimed. Which? Found that between June 2014 and May 2015, 37 million passenger journeys to and from the UK were by 15 minutes or more, with more than 900,000 people eligible for compensation. However, the consumer magazine fund only an average of 38 per cent of passengers made a claim. Any passenger delayed for more than three hours is entitled to up to L521 under the Denied Boarding Regulation...According to Which?, 30 per cent of flyers have experienced delays or cancellations with their flight with more than 9,000 flights delays for three hours or more each year. The magazine surveyed more than 7,000 of its members-it found half of those who had been delayed, received no support or information about the delay they experienced from their airline".

Airline Seats Antitrust Cases

In Reisinger, *Airline Seats Antitrust Case Heads for Takeoff*, www.corpcounsel.com (8/26/2015) it was noted that "More than 75 class action lawsuits have been filed across the country so far against the four major airlines that are the targets of an antitrust investigation by the Department of Justice, which is exploring whether the airlines kept ticket prices high by limiting the number of available seats. A federal judicial panel on multi-district litigation has scheduled an Oct. 1 hearing to consider requests to combine the cases before one federal court".

Serengeti Highway On Hold

In *East Africa court appeal affirms ruling against Serengeti Highway*, www.eturbonews.com (8/26/2015) it was noted that "In a recent decision...the Appeals Division of the Arusha-based East African Court of Justice upheld (in part) the ruling of the lower court in regard to a permanent injunction sought by the African Network for Animal Welfare...on behalf of the Tanzanian, East African and global conservation community...With the June 2014 decision now by and large standing, Tanzania will find it next to impossible to build a paved highway across the Serengeti's most

vulnerable migration routes".

Uber Wi-Fi In India

In Mozur, *Uber to Provide Free In-Car Wi-Fi in India,* www.nytimes.com (8/21/2015) it was noted that "In India, a country notorious for city-snarling traffic jams, Uber is hoping free in-car Wi-Fi will lure customers who don't want long transit times to take them offline...The company said in a news release that Bharti Airtel would operate the Wi-Fi through its new fourth-generation network in all 18 cities, including Mumbai, Delhi and Bangalore, where Uber operates. As part of the deal, Uber is also offering discounted cellphone plans for drivers and accepting payments using Airtel's mobile payment platform".

Travel Law Article: The Wyndham Case

In *Federal Trade Commission v. Wyndham Worldwide Corp.*, No. 14-3514 (3rd Cir. 2015) the Court of Appeals held "The Federal Trade Commission Act prohibits 'unfair or deceptive acts or practices in or affecting commerce'. 15 U.S.C. 45(a). In 2005 the (FTC) began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast

majority of these cases have ended in settlement".

The Security Breaches

"On three occasions in 2008 and 2009 hackers successfully accessed (Wyndham's) computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham's conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham's motion to dismiss, and we granted interlocutory appeal on two issues: whether the FTC has authority to regulate cybersecurity under the unfairness prong of Section 45(a); and if so whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision. We affirm the District Court".

Wyndham's Cybersecurity

"(Wyndham) is a hospitality company that franchises and manages hotels and sells timeshares through three subsidiaries. Wyndham licensed its brand name to approximately 90 independently owned hotels. Each Wyndham-branded hotel has a property

management system that processes consumer information that includes names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates and security codes. Wyndham 'manage[s]' these systems and requires the hotels to 'purchase and configure' them to its own specifications...It also operates a computer network in Phoenix, Arizona, that connects its data center with the property management systems of each of the Wyndham-branded hotels".

The FTC Allegations

"The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that 'taken together, unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft'...This claim is fleshed out as follows:"

Clear Readable Text

"1. The company allowed Wyndham-branded hotels to store payment card information in clear readable text".

Easily Guessed Passwords

"2. Wyndham allowed the use of easily guessed passwords to access the property management systems. For example, to gain 'remote access to at least one hotel's system' which was developed by Micros Systems, Inc., the user ID and password were both 'micros'".

Absence Of Firewalls

"3. Wyndham failed to use 'readily available security measures'-such as firewalls-to 'limit access between [the] hotels' property management systems,...corporate network and the Internet'".

Inadequate Policies-Out Of Date Systems

"4. Wyndham allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions. It did not ensure that the hotels implemented 'adequate information security policies and procedures'...Also, it knowingly allowed at least one hotel to connect to the Wyndham network with an out-of-date operating system that had not received a security update in over three years. It allowed hotel servers to connect to Wyndham's network even though 'default user IDs and passwords were enabled...which were easily available to

hackers through simple Internet searches'. And, because it failed to maintain an 'adequate[] inventory [of] computers connected to [Wyndham's] network [to] manage the devices', it was unable to identify the source of at least one of the cybersecurity attacks".

Failure To Restrict Access

"5. Wyndham failed to 'adequately restrict' the access of third-party vendors to its network and the servers of Wyndham-branded hotels. For example, it did not 'restrict[] connections to specified IP addresses or grant[] temporary, limited access, as necessary'".

Failure To Conduct Security Investigations

"6. It failed to employ 'reasonable measures to detect and prevent unauthorized access' to its computer network or to 'conduct security investigations'".

Improper Incident Response Procedures

"7. It did not follow 'proper incident response procedures'...The hackers used similar methods in each attack,

and yet Wyndham failed to monitor its network for malware used in the previous intrusions".

Overstated Privacy Policy

"Although not before us on appeal, the complaint also raises a deception claim, alleging that since 2008 Wyndham has published a privacy policy on its website that overstates the company's cybersecurity.

'We safeguard our Customers' personally identifiable information by using industry standard practices. Although 'guaranteed' security' does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such [i]nformation consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128-bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information-such as credit card numbers, online forms, and financial data-from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and

maintain ‘fire walls’ and other appropriate safeguards...’

“The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls and other commercially reasonable methods for protecting consumer data”.

First Cybersecurity Attack

“As noted, on three occasions in 2008 and 2009 hackers accessed Wyndham’s network and the property management systems of Wyndham-branded hotels. In April 2008, hackers first 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-repeatedly guessing users’ login ID and passwords-to access an administrator account on Wyndham’s network. This enabled them to obtain other consumer data on computers throughout the network. In total, the hackers obtained unencrypted information for over 500,000 accounts, which they sent to domain in Russia”.

Second Cybersecurity Attack

“In March 2009, hackers attacked again, this time by accessing Wyndham’s network through an administrative account. The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges.

Wyndham then discovered 'memory-scraping malware' used in the previous attack on more than thirty hotels' computer system...The FTC asserts that, due to Wyndham's 'failure to monitor [the network] for the malware used in the previous attack, hackers had unauthorized access to [its] network for approximately two months'. In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels".

Third Cybersecurity Attack

"Hackers in late 2009 breached Wyndham's cybersecurity a third time by accessing an administrator account of one of its networks. Because Wyndham 'had still not adequately limited access between...the Wyndham-branded hotels' property management systems, [Wyndham's network] and the Internet', the hackers had access to the property management servers of multiple hotels... Wyndham only learned of the intrusion in January 2010 when a credit card company received complaints from cardholders. In this third attack, hackers obtained payment card information for approximately 69,000 customers from the property management systems at 28 hotels".

The Damages Done

"The FTC alleges that, in total, the hackers obtained payment card information from over 619,000 consumers, which (as noted) resulted in at least $10.6 million in fraud loss. It further states that consumers suffered financial injury through 'unreimbursed fraudulent charges, increased costs, and lost access to funds or credit...and that they 'expended time and money resolving fraudulent charges and mitigating subsequent harm'".

Conclusion

All travel suppliers and resellers should take careful note of Wyndham's alleged failure to adequately protect its guests' personal information from hackers.

Justice Dickerson been writing about *Travel Law* for 39 years including his annually updated law books, *Travel Law*, Law Journal Press (2015) and *Litigating International Torts in U.S. Courts*, Thomson Reuters WestLaw (2015), and over 350 legal articles many of which are available at www.nycourts.gov/courts/9jd/taxcertatd.shtml. For additional travel law news and developments, especially, in the member states of the EU see www.IFTTA.org