porterwright

Restaurant and Hospitality Industry Alert

A Litigation Department Publication

January 2015

David Tryon
216.443.2560
dtryon@porterwright.com

Bob Tannous
614.227.1953
rtannous@porterwright.com

Please see our other publications at www.porterwright.com/pubs.

Cyber Security Liability in the Hospitality World

"I am glad we aren't Sony…

…or Target or Home Depot or Wyndham or TJX (Marshalls/T.J. Maxx) or Apple or Hannaford Brothers or Staples!" This is what many companies are thinking. Why? What do all of them have in common? They all had customers' personal data stolen (a "Data Breach"). And they all paid out hundreds of thousands or even millions of dollars as a result. Are you any different from them? You think, or hope, that you are – that your systems are either secure from attack or that you are not a likely target. But not only are you a likely target, hotels and hotel management companies can be hit especially hard by such attacks. Consider that while you might manage hotels in only one state, you have guests from many states. You collect credit card information and other personal information from all of your guests. Then, you are hacked!

No problem you think. First, the credit card holders don't need to pay for any fraudulent charges; the banks issuing the cards just absorb those, right? *Wrong.* Second, I don't need to notify anyone since it wasn't that big of a deal. *Wrong again.* But, you say, even if I have to do a notification, I just worry about the laws of the state where my management company is located. *Wrong yet again*. Even so, you respond, at least I only have to worry about dealing with the state government and not any of those class actions I have heard about! *Not anymore*. Finally, at least I don't have to worry about the feds, there are no federal laws on that. *Well, not exactly right*. Fortunately, you say, my general commercial insurance should cover me. Sorry to say, no it does not — unless you purchased a special endorsement for that.

First, the credit card protections: While it is true that your guests are protected from credit card fraud by the terms of the credit cards, it is not true that the issuing banks absorb the losses. They recover much of those losses through increased card fees and increased rates, but they have another potential recovery: "subrogation." This means that the banks take whatever rights their cardholders might have against other businesses for the losses the banks sustain. So, the banks can take action against a hotel or management company that did not keep the private information secure if the hotel/management company was negligent. For example, TJX Companies Inc. (owner of Marshalls, T.J. Maxx and others) and MasterCard International Inc. reached a $24 million settlement with banks that issued MasterCard cards which were compromised in a Data Breach. Obviously, the damages can be huge.

Second, 47 states now have Data Breach Notification laws. Ohio's law is typical.

It requires that the business quickly notify (no later than 45 days after learning of the data breach) each Ohio resident whose personal information was stolen. (See details at O.R.C.§1349.19.) The state of Ohio can sue the business for failure to comply. Penalties are $1,000 for failure to comply for the first 60 days of violations and increase to as much as $10,000 per day.

But the story does not end there. If your hotel has guests from other states, you have to comply with the Data Breach Notification Laws of all those states. So you need a response policy (see below) that complies with all state Data Breach Notification Laws to make sure you are complying, or you risk the statutory penalties of each those states' laws.

Class actions are another danger. If you know anything about class actions, you know that they are expensive to defend and that they last for years. You may have heard that courts have rejected class actions for these kind of claims; and that *was* true at one time. But this isn't true anymore. Most recently, Sony has been sued in a class action in California. *Corona, et al. v. Sony Pictures Entm't, Inc.*, Case No. 2:14-cv 09600 (C.D. Cal. 2014). In 2008, 16 class action lawsuits were filed against Delhaize America, Inc. for Data Breaches at its retail store subsidiaries. *In Re: Hannaford Bros. Co. Customer Data Safety Breach Litigation*, Case No. 2:08md1954 (U.S. Dist. Maine 2008). The Virginia Veterans' Affairs Department was sued in a class action for loss of 26.5 million veterans' personal information. *Kennedy v. U.S. Dept. of Veteran's Affairs,* Case No. 1:06cv1070 (D.C. Cir. 2006). One of the TJX cases referenced above was also a class action suit. If you have a Data Breach, you should expect a class action suit.

As you may have heard from one or more trade groups, there have been attempts to pass Federal Data Breach Notification Laws. Those efforts have failed so far. But that has not stopped the newly aggressive Federal Trade Commission ("FTC") from taking action. The FTC has decided that (to paraphrase recent political statements) if Congress won't act, they will. The FTC is now attacking some companies who themselves have been victims of Data Breaches. Once a Data Breach occurs, the FTC steps in and claims that the company's failure to protect the information is an "unfair trade practice" and enforces data-security standards hitherto unknown to the business. For example, in 2012, the FTC sued Wyndham Hotels claiming that Wyndham "failed to employ reasonable and appropriate measures to protect information against unauthorized access." The FTC claimed a violation of Section 5 of the FTC Act (15 U.S.C. §45(a) and (n)) Wyndham moved to dismiss on the grounds that the FTC lacks the authority to regulate cybersecurity and that the FTC failed to provide notice of what cybersecurity practices it was requiring. The trial court denied that motion and an appeal is pending on that issue. *FTC v. Wyndham Worldwide Corp*., Case No. 14-3514 (3d Cir. 2014). The FTC has asserted these types of claims over 20 times.

As you might guess from the foregoing, the cost to deal with a Data Breach is high. It is not unusual for the cost to be about $100 *per record – or more*. Imagine if the data for all your guests from the past 10 years were compromised! This is not a pretty picture.

We are all tempted to say, "This cannot happen to me." That is what Sony, Home Depot and others thought, and we know what happened to them. The public, the courts and the federal government are increasingly subscribing to former FTC Chair Deborah Platt Majoras' statement: "By now the message should be clear: companies that collect sensitive consumer information have a responsibility to keep it secure."

Is there any good news? Yes there is. You can protect yourself. Here are several suggestions:

- Get data security insurance coverage to cover these types of losses. Available insurance coverages include (a) "Identity Recovery" to help identify theft victims restore the victims to pre-theft status, (b) "Date Compromise" to pay for required postdate notifications and (c) "Cyber One" to protect against business losses from damages to your computer systems and from claims made by guests (and others) damaged by a Data Breach.

- Re-evaluate your data protection policies and technology. Technology changes. The law changes. Employees come and go. Are you up-to-date? Ignorance of the technology or law is no excuse, and failure to train employees will guarantee trouble.

- Establish a Rapid Response Policy. Like all emergencies, there is little time to think when a data breach occurs. It is not a question of if, but when and how big. It may be one record caused by a bad employee or it may be a major system hack. So, expect it and plan for it. Designate a decision-maker and a spokesperson. Find a qualified lawyer and IT specialist who will help respond when the time comes. Determine which state laws you will have to comply with, how the notices will be sent and if you need a customer call center. Find

out what ID theft insurance and credit watch services might be helpful to offer affected guests. Is this annoying? Yes. But it could be the difference between the preservation and demise of your business when it happens.

- Comply with state laws. If you have a Data Breach, give the required statutory notice quickly.
- Fight back. The media, the public and some government officials assume that if data is compromised that the business has been negligent and the business is liable. That is not so. While public relations dictates helping your customers, it does not preclude actively defending against class actions, government enforcement action or other attempts to establish legal liability. Sometimes rolling over and paying money is the cheapest short term solution, but it is not always the best long term solution. A settlement with the FTC may result in unacceptable long term compliance costs and monitoring. Settling a class action suit prematurely can result in overpayment and excessive rules and regulations. As you analyze legal actions, consider short and long term costs, and their perception by future government enforcers and class action plaintiffs' attorneys.

Our cyber world provides opportunities and pitfalls. Take advantage of the former, but prepare for the latter.

David Tryon and Ben Bowers prepared this article for the hotel and lodging industry. David is a partner at the law firm of Porter Wright Morris & Arthur LLP and can be reached at (216)443-2560 and dtryon@porterwright.com. Porter Wright has created a 50 State Matrix of Data Breach Laws that it has used to help protect businesses from cyber-attacks and protect them from legal claims based on cyber-attacks. Ben Bowers is president of Bowers Insurance Group, which has been providing property and casualty insurance to the hospitality industry for over 20 years.