More Than an Upgrade

Payment Card Industry Data Security Standards

By Callie E. Waers

Among other things, these standards can help retail and hospitality companies to manage data breach-related liability and to comply with payment card contracts with processing bank contracts.

The Payment Card Industry Data Security Standards (PCI DSS), developed by the PCI Security Standards Council, are a set of 12 requirements that are designed to create a minimum level of secure data management practices for banks and vendors that accept and process payments using payment cards. Most retail and hospitality companies process hundreds to thousands of payment card transactions each day, yet many of these companies do not comply with these standards. Even worse, many of the companies that are not compliant do not even realize it.

Retail and Hospitality Organizations Are Attractive Targets

Retail and hospitality companies are extremely attractive, data-rich targets for cybercriminals, and it is important that their leaders and lawyers know why. Hospitality and retail companies are now, more than ever, providing interactive guest experiences. As technology advances facilitate an increase in interaction, there is a corresponding increase in entry points to and vulnerability among these companies. By their nature, these companies have a higher transaction frequency than companies in many other industries. High transaction turnover is valuable because of the increase in opportunity. Payment card data collected in transit is active and more likely to be valid and more valuable to cybercriminals than older stored data. Another point to consider when weighing the value of these industries' data is that hospitality and retail companies process expendable income transactions more often than other industries.

The risk grows because hospitality and retail companies, unlike those in the health and finance industries, do not typically believe that they possess sensitive and confidential data. Therefore, the typical front-line service worker has generally received little, if any, training on data safety. In some cases, having a simple awareness of the problem may be the first step to a solution. Some of the most glaring errors in security have simple fixes such as not using software default passwords, or not using common passwords. Hospitality and retail companies also frequently provide public Wi-Fi networks for their customers to use,

■ Callie E. Waers is an associate in Babst Calland Clements and Zomnir PC's Charleston, West Virginia, office. Ms. Waers has represented clients in cases dealing with a wide variety of legal issues, such as professional liability, insurance coverage, personal injury, construction disputes, constitutional and civil rights claims, privacy law and data breach matters, and issues arising under the Health Insurance Portability and Accountability Act (HIPAA).

© 2016 DRI. All rights reserved.

which can create dangerous points of entry. These characteristics not only make these companies attractive to malevolent actors, but they are the very reason that these companies need to be more aware of the steps that they need to take or have not taken to guard sensitive data.

Trustwave, an information security and compliance solutions company, issues an annual *Global Security Report* that addresses security shortfalls and collects learning points from the previous year's breaches. The most recent report listed the top-three industries that experienced compromises in 2014 as retail, food and beverage, and hospitality. The retail industry experienced an increase in breaches from 35 percent in 2013 to 43 percent in 2014. The crucial takeaways from Trustwave's report are as follows: (1) retail companies experience more frequent e-commerce asset attacks than other attack types; (2) most hospitality and food and beverage company attacks happen at point-of-sale (POS) locations; (3) generally, North American companies experience more POS attacks than attacks to e-commerce or corporate network assets; and (4) the methods of intrusion were most commonly weak passwords or weak remote access security. These points of vulnerability combined with the attractiveness of hospitality and retail companies as data targets create a serious risk of data breaches that can open companies up to numerous legal issues.

Some of the most glaring errors in security have simple fixes such as not using software default passwords, or not using common passwords.

There are several key ways that a company can be held liable after it experiences a data breach. A company can face civil liability under the Federal Trade Commission Act (FTC Act), consumer lawsuits for negligence, and bank lawsuits for breach of contract. Data breach notification laws govern an organization's conduct after a breach, but those laws will not be addressed in this analysis.

FTCA Liability Under Section 5

The Federal Trade Commission (FTC) has used Section 5 of the FTC Act to regulate data mismanagement between vendors and their customers. The FTC Act gives the FTC jurisdiction to prevent "persons, partnerships, or corporations… from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. §45(a). Section 5 of the FTC Act declares "unfair or deceptive practices in or affecting commerce" unlawful. *Id.* This language has been used to bring actions against companies for violating their own privacy policies as well as poor management of consumer personally identifiable information (PII). The FTC uses the following criteria in assessing when to investigate a case based on deception: (1) there must be a representation, omission, or practice that is likely to mislead the consumer; (2) the practice is examined from the perspective of a consumer acting reasonably in such circumstances; and (3) the representation, omission, or practice must be material in that it is likely to affect a consumer's conduct or decision regarding a product or a service. 103 F.T.C. 110, 174 (1984).

Two famous examples of hospitality and retail breaches help to understand FTC-imposed civil liability. First, in early 2007, TJX Companies, Inc., a well-known retailer, announced that millions of consumers' payment card information had been compromised as a result of a data breach. The resulting harm affected not only the consumers, but also the banks that issued the compromised cards. By the time that the banks that issued the payment cards finished investigating the breach, they speculated that over 94 million credit cards had been compromised since 2005 when the breach initially started. The FTC brought a Section 5 complaint against TJX, which outlined the issues that it believed amounted to unfair acts or practices. Specifically, the complaint said that TJX stored and transmitted payment card data in clear text, or unencrypted form; did not limit access to in-store wireless networks; failed to use a firewall to limit remote access to computers; and failed to use any monitoring, prevention, or detection methods. *In re TJX Companies, Inc.,* FTC File No. 072-3055, at 2–3 (Mar. 27, 2008).

The second case involved a hospitality company. In *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015), the Third Circuit recently addressed whether or not the FTC had the authority to regulate cybersecurity under 15 U.S.C. §45(a). Wyndham Worldwide Corporation experienced three serious data breaches in 2008 and 2009 that resulted in over $10 million in fraudulent charges. The court found that the FTC has the authority to regulate unfair acts or practices as long as an act or a practice (1) "causes or is likely to cause substantial injury to consumers"; (2) the injury "is not reasonably avoidable by consumers"; and (3) the injury "is not outweighed by… benefits to consumers or to competition." *Wyndham Worldwide Corp.*, 799 F.3d at 244. Liability under the FTC Act results from mismanagement of PII resulting from an unfair, misleading practice or a misrepresentation to consumers. The mismanagement of PII is usually predicated on a failure to implement standard cybersecurity measures, such as encryption, fire walls, and unique passwords.

In *Wyndham*, the FTC originally raised a deception claim that alleged that Wyndham overstated its cybersecurity in its website's privacy policy. *Id.* at 241. Specifically, Wyndham's policy stated that it used industry-standard practices, including "fire walls" and encryption. *Id.* The FTC alleged that neither firewalls nor encryption were used.

Breach of Contract and Indemnification

There is a complicated arrangement of parties in commercial payment card data breaches. Usually, a breach of contract claim can be brought by a processor that paid a fine to a payment card company. Typically, neither a consumer's bank nor the vendor that experiences a breach is a signatory to the payment card contract that requires compliance with the PCI DSS, or Payment Card Industry Data Security Standards. The payment card companies contract with the processing banks used

by vendors, and they require those banks to ensure that the vendors are PCI DSS compliant. This relationship was illustrated in the TJX Companies, Inc. data breach in 2007, in which the banks that had to compensate consumers for fraudulent use were not parties to the contracts between the payment cards, processing banks, and vendors. The banks could not recover for breach of contract without being a party to the contract or a third-party beneficiary. *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 499 (1st. Cir. 2009) (finding the banks could only bring breach of contract claims if they were third-party beneficiaries and that each agreement between TJX and their processing banks stated that it was only to the benefit of the parties to the contract).

Another good illustration of the complicated arrangement of parties in litigation resulting from PCI DSS noncompliance can be found in *Genesco, Inc. v. Visa U.S.A., Inc.*, 296 F.R.D. 559, 561 (M.D. Tenn. 2014). In *Genesco*, the payment card company, Visa, sought over $13 million in fines from a processing bank predicated on noncompliance with the PCI DSS. The processing bank sought indemnification for the fines from the vendor, Genesco, under the processing contract between the bank and vendor. In turn, the processing bank assigned any claims against Visa to Genesco. Genesco sued Visa as the assignee and subrogee of the processing bank, disputing Visa's factual basis for the PCI DSS violations. Trustwave conducted a forensic investigation of the cyberattack, and it determined that Genesco was not compliant with three of the 12 PCI DSS requirements.

Given the complicated nature of the relationships and parties involved in payment card data breaches, litigation can be time-consuming and involve multiple stages. Further, because this litigation deals with electronic discovery and often some degree of forensics, it can be quite costly.

Negligence

Liability for negligence for data breaches greatly depends on the jurisdiction. However, simply being exposed to a breach is generally not sufficient to establish a *prima facie* case of negligence. Most jurisdictions require actual damages to be present to succeed on an action for negligence in data management. The economic-loss doctrine typically bars recovery for purely economic loss in tort actions, and some courts have held that the doctrine bars recovery for breach, or exposure to potential loss, without evidence of damages.

In *Paul v. Providence Health-System-Oregon*, a case decided in Supreme Court of Oregon in 2011, the court examined how the economic-loss doctrine would operate in a data breach case. 351 Or. 587 (Or. 2011). In *Paul*, protected health information was stolen from a health-care provider. The information was not used, but the patients brought a class action alleging common law negligence. The court noted that damages were available to the plaintiffs if they could prove that the defendant had a "duty to guard against the economic loss that occurred." *Id.* at 593. The court distinguished this duty from the duty that common law negligence places on persons in general, but the court limited it to a duty arising from relationships or legislation. While the court declined to decide if the defendant owed this duty to the plaintiffs in the case, it did say that even if the defendant did, the plaintiffs' allegations were "insufficient" because they did not allege "actual, present injury caused by defendant's conduct." *Id.* at 594. The court seemed willing to entertain an exception to the economic-loss rule but not in cases involving only future harm.

Some plaintiffs make the argument that compensation for credit-monitoring enrollment as a result of a data breach is analogous to compensation for medical monitoring in toxic exposure cases. This argument is not always well received by the courts. The difference in most cases seems to be that courts appear to recognize a public policy argument that supports health monitoring, but they do not recognize one that supports credit monitoring. In *Providence Health System*, the plaintiffs made this exact argument, and the court declined to analogize medical monitoring cases to credit monitoring because "requir[ing] defendant here to pay for credit monitoring because of the increased *risk* of a purely *economic* future harm would require an even greater departure from existing case law." *Id.* at 594. The distinction between present and future harm when it comes to data breaches definitely raises the bar for plaintiffs to bring negligence claims of purely economic loss when they do not experience further fraudulent use of the data.

Some states, however, do not require an actual injury. West Virginia, for example, recognizes a legally protected interest in privacy that it has found to be actionable even though a plaintiff does not allege special damages. *Tabata v. Charleston Area Med. Ctr., Inc.*, 233 W. Va. 512, 759 S.E.2d 459 (W. Va. 2014). West Virginia is aligned with Oregon in *Providence Health System* in finding that a risk of future identity theft is not actionable, but it found that plaintiffs whose information was accidentally published on a website but who presented no evidence of malicious use had a valid invasion of privacy claim. *Tabata*, 233 W. Va. at 512. Each jurisdiction handles consumer tort claims against vendors differently, but once damages are dealt with, the next hurdle that litigants confront becomes the security protocol levels or maintenance of those protocols that is viewed as so inadequate as to breach a duty of reasonable care.

There is a complicated arrangement of parties in commercial payment card data breaches.

PCI DSS

The payment card industry has taken initiative to prevent fraudulent credit activity as a result of cybercrime by implementing the PCI DSS, or Payment Card Industry Data Security Standards, which contractually obligate all processing banks and vendors that accept major payment card transactions to abide by certain security standards.

The standards are divided into 12 steps, each of which includes much more complicated steps to implement. To be PCI DSS compliant, vendors must (1) maintain a firewall; (2) change default passwords; (3) protect stored card data; (4) encrypt transmissions; (5) update anti-

virus software and protect against malware; (6) develop and maintain secure systems and applications; (7) restrict card data access to business need-to-know purposes; (8) identify and authenticate access to system components; (9) restrict physical access; (10) monitor and track network access; (11) regularly test security; and (12) maintain an internal security policy.

Another critical breeding ground for data vulnerability is a knowledge deficit among employees.

The requirements require monitoring access and developing unique passwords, solutions to two major areas that affected hospitality and retail companies greatly in 2014. Critically, the requirements mandate periodic review and documentation, something that risk managers know is critical. The 12 steps are designed to be their own safety net, and if they are implemented properly, they can serve as useful tools in preventing, or at the very least, quickly identifying weaknesses or breaches.

Implementation Challenges

The costs of implementing these 12 requirements can be staggering. Many companies ranging from international chains to single property restaurants and hotels had to upgrade software to become compliant in 2013 when the new PCI DSS (Version 3.0) went into effect, an operationally and financially burdensome change. As recently as April 2015, the standards were updated again, and the most current version is PCI DSS Version 3.1. The standards required some companies to make software upgrades (and sometimes hardware upgrades) and to institute new information technology protocols. Depending on the size of the company and its operating budget, these upgrades can have a significant cost, both monetary and staffing related. When it comes to PCI DSS compliance, it is easy to focus on the big ticket items such as compliant software, but the solution is usually not just an upgrade.

Vulnerability arises when the PCI standards are not followed as they are intended to be. Trustwave's 2011 Global Security Report outlined many of the major problems with PCI DSS compliance discovered by its investigations in 2010. *Trustwave 2011 Global Security Report,* Trustwave (Feb. 13, 2012). One area of vulnerability for many companies is the software that they use to manage their information. In the case of a hotel, for example, the property management system (PMS) purchased may be advertised as "PCI DSS compliant" because it is equipped to guard information in a manner that complies with the PCI DSS. However, simply upgrading to a compliant PMS will not guard a hotel against security intrusions, and similarly, it will also not make a hotel compliant with the standards. The system will have options that must be configured correctly, and a hotel must take ongoing steps. Although a property management system may be entirely compliant, if it is not guarded by a firewall, a hotel using it is actually not compliant with the standards. Other user-controlled aspects of software that affect compliance are the use of default or vendor-assigned passwords and the assignment of unique identifications for each user with access to a system. In addition, some of the most overlooked elements of compliance are simply tracking network access and regularly testing security. Software vendors have no control over the execution of many of these requirements, so to purchase a "PCI DSS-compliant" system can be misleading.

Another critical breeding ground for data vulnerability is a knowledge deficit among employees. As mentioned before, employees in typical retail and hospitality establishments generally do not view themselves as working in a field that involves highly confidential information. In contrast, the Health Information Portability and Accountability Act (HIPAA) requires yearly training on HIPAA policies and procedures designed to safeguard sensitive data, and the health-care and finance industries are regulated in a manner that creates a culture of confidentiality. Now more than ever, all companies that handle personally identifiable information, such as the PII handled by companies in the retail and hospitality industries, should train employees on data safety and how to use software features that ensure safe data management practices.

A New Perspective

While it is clear that noncompliance with the PCI DSS can have legal consequences, perhaps the standards should be viewed by vendors as a shield rather than a sword. The PCI DSS requirements address major concerns for hospitality and retail companies, such as weak passwords and weak remote access controls. Making compliance a priority and creating a culture of data safety among employees not only assists in protecting customer data, but it also can protect a company from liability for fines related to noncompliance. Moreover, PCI DSS compliance is, in essence, compliance with industry standards, which assists with the defense of negligence claims from consumers, when it is allowed.

In December 2015, the FTC settled its civil action against Wyndham, and the Stipulated Order offers support to the theory that PCI DSS may potentially be used as a shield to liability. The Stipulated Order refers to PCI DSS as the "Approved Standard," and it requires the company to obtain a written assessment of compliance with the Approved Standard annually. The FTC's use of PCI DSS compliance as an assessment of Wyndham's data safety practices further suggests that PCI DSS may operate as a practical shield to liability from ever-increasingly complicated privacy laws and regulations.

To tackle the FTC Act liability, transparency and consistency are crucial. Good risk management practices will ensure that a company's privacy policy is consistent with the PCI DSS, and more critically, will ensure that the privacy policy is consistent with company practices. Consistency between a privacy policy and actual practices greatly reduces risk that a misleading representation that would violate the FTC Act would reach consumers, and making both a company's privacy policy and standards consistent with the PCI DSS requirements would ensure that the company uses industry standards. The added benefit of these industry standards is that they assist companies to comply with processing bank contracts. It is a win-win for everyone. FD