Craig R. Tractenberg and Keri McWilliams, The Legal Intelligencer

October 31, 2014 | 0 Comments

share

- share by mail
- share on linkedin
- Facebook
- share on twitter
- share on google+

Share With Email

RECIPIENT, SEPARATE MUL

Add a comment...

Send

Thank you for sharing!

Your article was successfully shared with the contacts you provided.

print
reprints

Data breaches at Target, Home Depot, Neiman Marcus and P.F. Chang's are front-page reminders of the vulnerability of customer payment information in the retail sector. Verizon estimated that "74 percent of attacks on retail, accommodation, and food services companies target payment card

information." In *Federal Trade Commission v. Wyndham Worldwide*, Case No. 13-cv-01887 (D. N.J. 2014), the Federal Trade Commission (FTC) brought suit claiming that a franchisor's alleged failures to maintain reasonable security measures constituted unfair and deceptive practices under Section 5 of the FTC Act. Although the FTC is clear about what the franchisor allegedly did wrong (failed to employ commonly used methods of data protection, such as complex passwords, network inventories and firewalls), little guidance exists from the FTC to help franchisors determine what standards are reasonable.

## What We Can Learn From Credit Card Companies

In 2006, five major credit card brands (Visa, MasterCard, American Express, Discover Financial Services and JCB International) formed the Payment Card Industry Security Standards Council to address issues of credit card payment security. The security council ultimately promulgated the Payment Card Industry Data Security Standard, or PCI-DSS for short. PCI-DSS is a set of standards developed to ensure the security of all credit card payment information handled by merchants. The standards are intended to apply to any business that processes, transmits, or otherwise handles credit card transactions. Accordingly, these standards are applicable and relevant for franchisors and franchisees alike. Although all companies that accept credit cards are required to be PCI-compliant, a significant percentage of businesses fail to understand their PCI-DSS obligations. For franchise systems, the consequence of a data breach involving credit cards, even if limited to an individual franchise, can be very damaging both in dollars and brand good will. And that threat will only increase. The August 2013 Nilson Report estimated that total global payment-card fraud losses were $11.3 billion in 2012.

## Requirements of PCI-DSS

PCI-DSS was designed to specifically address vulnerabilities that lead to credit card data loss. The most recent update is PCI-DSS Version 3.0, which became effective Jan. 1, and is mandatory beginning Jan. 1, 2015. The PCI-DSS regime consists of six general areas of concerns and 12 distinct standards as follows. The areas of concern include building and maintaining a secure network and system, maintaining a vulnerability management program, and regularly monitoring and testing networks. A full list can be found at http://goo.gl/TdICcg.

## The Franchisor's PCI-DSS Obligations

In order to accept credit cards and become part of payment card networks, merchants such as franchisees and franchisors must work through and contract with a bank (merchant bank). The contracts with the merchant banks typically require all merchants to comply with PCI-DSS standards but, for franchisors, the scope of that requirement can vary significantly depending on the volume of credit card transactions that the franchisor handles, and the relationship between the systems of the franchisors and the systems of the franchisees.

Each credit card brand mandates specific PCI compliance reporting and validation requirements depending on the volume of transactions processed by a merchant each year. For example, Visa's largest "Level 1" merchants, which are those processing more than 6 million Visa transactions a year, are required to (a) prepare and submit an annual report on compliance conducted by a qualified security assessor (or an internal auditor, if signed by an officer of the merchant), (b) complete a

quarterly network scan by approved scan vendor, and (c) complete an attestation of compliance. In contrast, Visa's smallest "Level 4" merchants, which are those processing less than 1 million Visa transactions a year and less than 20,000 e-commerce transactions, are only required to complete an annual self-assessment questionnaire and a quarterly network scan, although the merchant bank may impose additional requirements. Each credit card brand determines its own tiers and validation requirements.

Because PCI-DSS requires franchisors to assess and comply with PCI-DSS standards for all systems that are connected to any database in which payment card information is processed or stored, the cost and scope of PCI compliance also varies based on the connectivity of a franchise system. As the franchise model and technology evolve, more and more franchisors are connected to their franchisees' management systems to provide remote management services, administer loyalty programs, provide centralized reservations, validate receipts, or allow franchisees to connect to the franchisor intranet. In some franchise models, the franchisor may actually process credit card payments on behalf of its franchisees. Each layer of connectivity can add to the scope of the franchisor's PCI compliance obligations, the costs associated with compliance, and the scope of its potential liability.

# The Consequences of Failure

Franchisors and franchisees may face liability from their customers if information is compromised. Minnesota and Nevada have mandated that certain companies serving the residents of those states must comply with at least certain portions of the PCI-DSS requirements. Private litigants may point to noncompliance with PCI-DSS as evidence of a failure to maintain a reasonable standard of care.

Federal liability is also possible. In *Wyndham*, Wyndham challenged the FTC's enforcement authority related to data breaches. However, the U.S. District Court for the District of New Jersey refused to the dismiss the FTC's action against Wyndham Worldwide Corp. for its alleged "failure to maintain reasonable security" after hackers were able to access credit card account numbers and security codes on the computer networks of Wyndham Hotels and Resorts, including several hotels in its franchise network. The case is still pending.

# Best Practices for Franchisors

• **Assess the system.**

If a franchisor has not been carefully complying with PCI-DSS, now is the time. Third-party vendors can help you assess the problem. The questions to ask are: What are all of the ways in which payment information is processed and stored? Does the franchisor mandate a specific POS system for all franchisees? If so, is the POS system and installation process PCI-compliant? If not, what protections are in place to ensure that the systems that franchisees choose are PCI-compliant? Is the customer payment data on the franchisor's system protected by a firewall and segregated from other portions of the franchisor's network? Is customer payment data on franchisees' systems similarly protected? Does the franchisor or any franchisees retain customer payment information? If so, is such retention really necessary? Is any payment information encrypted and protected adequately? How connected is the franchisor to the franchisees' system? If the connection is an always-on connection, is that necessary? Can customer information be accessed by mobile devices? If so, are those adequately protected?

• **Develop a data privacy policy and update your franchise agreements and operations manuals to reflect your requirements.**

After a franchisor has assessed and addressed any issues in its own system, it should develop reasonable data-protection policy for its franchisees. At minimum, the franchise agreement should require that franchisees maintain PCI compliance and comply with any applicable data-protection laws. For franchisors, the best practice is to require that franchisees be PCI-DSS-compliant, and to provide resources and support to help them achieve compliance. Franchisors should explain PCI-DSS obligations in their training. Franchisors should ensure that any POS systems designated by the franchisor are PCI-compliant, and that franchisees have installed the necessary firewalls and protection. While mandating specific POS systems and data privacy standards may increase the potential for vicarious liability in the event of a data breach, failing to provide any direction or training to franchisees regarding their credit card data privacy obligations significantly increases the likelihood that a breach may occur in the first place.

• **Be vigilant.**

The Verizon 2014 PCI Compliance Report found that "organizations that suffered a data breach were less likely to be PCI-DSS-compliant at the time of their breach—even if compliant at the time of their last assessment—than the average of companies assessed." Essentially, even if systems comply with annual reporting requirements, it is easy to get out of compliance between annual assessments. Regular compliance reminders and checks can decrease the likelihood of a breach. The franchisor should ensure that PCI-DSS standards are included in its general system compliance policy and that its franchise operations team can assess potential PCI concerns in its regular inspection program. Simple changes such as requiring complex passwords, requiring regular changes to passwords, limiting access to sensitive information, maintaining firewalls, and updating antivirus software (all PCI-DSS requirements) can significantly increase the safety of the systems of both franchisors and franchisees. As part of a comprehensive data-privacy policy, franchisors should consider providing or requiring third-party assessments of franchisee systems on a regular basis.

While the steps above may seem daunting, preventing a data breach is much simpler than dealing with the fallout after one has occurred. In addition, there are vendors available that can assist franchisors with most stages of the compliance process. The wise franchisor should address compliance now to ensure continued brand protection.

***Craig R. Tractenberg*** *is the team leader of the franchise practice at Nixon Peabody and an adjunct professor of franchise law at Temple University's Beasley School of Law.* ***Keri McWilliams*** *is a franchise attorney with the firm. She counsels franchisors on domestic and international regulatory compliance and transactional issues.* •