

Articles / Whitepapers

Practice: Technology

Topic: PCI Compliance

PCI Compliant?

Hotels must join the battle against identity thieves and hackers, or pay the price. So says: Visa, American Express, MasterCard...



By Mark G. Haley

The credit card industry has a simple and straightforward message for every hotel and any other merchant who accepts credit cards: "If you don't have PCI now, get it fast, or else you'll regret it."

It is tough love from Visa and company, and your hotel cannot ignore it. The issue is the Payment Card Industry, Data Security Standard, often abbreviated as PCI DSS. The PCI DSS has been around since 2005, but countless merchants, including hotels, simply haven't gotten the message that if you accept credit cards in this age of cyber-crime, the merchant needs to defend against hackers and identity thieves.

Such defenses will cost time, effort and money, but the consequences of ignoring the PCI DSS will cost much more.

"PCI DSS compliance has become the elephant in the room," observes Chris Zoladz, vice president of Information Protection & Privacy for Marriott International. "PCI has raised the stakes and made protecting customer data prescriptive, not optional."

All merchants that accept credit cards are currently required to be in compliance with the PCI DSS. But the card issuers are enforcing compliance with varying reporting deadlines and validation requirements throughout 2007. Enforcement and compliance are very sensitive issues within the payment card industry. Yet, I find in my consulting work that most hoteliers are ill informed as to what PCI DSS is, why the hotel must comply, and what the hotelier needs to do about it.

What do PCI, PCI Data Security Standards, and PCI Compliance mean?

PCI, or Payment Card Industry, is a consortium of the major credit card companies who have come together to foster improved security of payment card information and trust in the global payment system. Members include Visa International, American Express Company, Discover Financial Services, MasterCard Worldwide and JCB.

PCI Data Security Standards are a set of 12 major standards comprised of over 200 specific requirements established by the PCI that establish minimum standards of security for both paper and electronic transactions and reports of transactions. It is sometimes abbreviated as PCI DSS, or simply DSS.

PCI Compliance refers to the extent that a given merchant, such as a hotel, restaurant or retailer, complies with the Data Security Standards.

The standards are owned and maintained by the PCI Security Standards Council, established and controlled by the PCI members. Enforcement of the standards is done by each individual card-issuing brand.

Why should a hotelier care about the PCI Data Security Standards? Because the merchant agreement a hotel uses to enable it to accept credit card transactions requires current adherence to the DSS, as well as, all future variants of the standard. All merchants that accept credit cards are required to comply, no matter how many or how few card transactions they process. PCI DSS is not a law; it is self-regulation by the payment card industry.

The credit card companies enforce the standards by imposing fines, which are then passed onto the merchant by their credit card merchant-services acquirer. The fines can be substantial, ranging from Visa's \$5,000 to \$25,000 per merchant per month to \$50,000 to \$200,000 by American Express. In 2006, Visa fined acquirers \$4.6 million for non-compliance. Hoteliers should expect more aggressive enforcement of proof of compliance going forward.

Does a property have to change all of its computer systems in order to comply?

The first task is to determine whether or not the computer systems are PCI compliant. Keep in mind, the merchant is responsible for compliance—not the vendors, not the brand, and not the owner. Every computer system in the hotel that stores credit card numbers must be evaluated, including the Property Management System, Point of Sale System, parking, spa and other applications. A wide range of third-party systems that might not be in the hotel must also be evaluated, such as, the Central Reservations System, the Internet Booking Engine, any Third-Party Intermediaries (Expedia, Travelocity, et al), and so on. The data network, and how it is connected to the outside world, also needs to be evaluated for compliance.

What else is necessary to comply? The business processes that involve payment card data, particularly reporting and records retention need to be examined. All reports and other paper that might have card data on them need to be secured and destroyed in a timely manner. For example, this might include hotel registration cards that have an imprint on the back. It is better to forego these imprints and rely on the card swipe data in the PMS. It is also necessary to engage an approved scanning

vendor to conduct quarterly network scans of the data network, and examine how it is connected to the outside world.

Finally, it is important to report the ongoing compliance efforts to the property's merchant services acquirer.

How does a property get this done?

- Appoint someone to be in charge of managing PCI compliance for the organization and make it part of their job, with dedicated time to do it.
- Enlist the support of the credit card merchant-services acquirer, the franchisor (if any), and other vendors.
- Require written statements regarding PCI compliance from all computer system vendors and distribution channels in use.
- Assess the "merchant level" for each card company to understand the compliance reporting requirements.
- Download and execute the PCI Self-Assessment Questionnaire.
- Address any deficiencies found in the Self-Assessment and repeat.

Where is the best source of information? The most authoritative Web site for PCI data is the PCI Security Standards Council (www.pcisecuritystandards.org). There you can find and download: the DSS document, the Self-Assessment Questionnaire, a list of computer systems validated to be compliant with the PCI DSS, and lists of approved scanning vendors and qualified security assessors.

A merchant services provider (credit card acquirer) is an essential resource in documenting compliance. It is essential to reach out to the service provider.

The merchants' section of the Visa Web site is also a rich resource (http://usa.visa.com/merchants/risk_management).

Finally, the IT system vendors can be useful partners in the compliance journey. ■

Mark G. Haley, CHTP, is a partner with The Prism Partnership LLC, a Boston-based consultancy servicing the global hospitality industry. Haley also serves as chairman of the AH&LA Technology Committee. He has deep experience in all aspects of hospitality technology and operations, including credit card processing. For more information, please visit: <http://theprismpartnership.com> or call 978-521-3600.

Article first published in the - New England Hotel Magazine