

Articles / Whitepapers

Practice: Technology

Topic: PCI Compliance

New Cards in the PCI Wallet

Hoteliers have - or have not - been listening to the imperatives delivered by all of the major credit card issuers known as "PCI Compliance" since 2005.



By Mark G. Haley

Lodging has covered PCI in detail before (see *It's in the Cards*, May 2007, by Mark G. Haley). However, the standards defined in PCI have been evolving, with the recent release of a new version of the standards, and Visa has published an updated, aggressive enforcement strategy aimed specifically at the computer systems that process credit card transactions. These new developments warrant a fresh look at PCI, so in this issue, we will:

- Briefly define PCI (Payment Card Industry Data Security Standards) and PCI compliance
- Recap the changes in version 1.2 of the PCI standards compared to version 1.1
- Discuss the recently-released "Payment Application Data Security Standards", or PA-DSS and the enforcement of these standards, the impact of them on vendors of computer systems and the hotel companies that buy them.

PCI and PCI DSS Defined

The Payment Card Industry Security Standards Council (PCI SSC; <https://pcisecuritystandards.org/>) is a non-profit organization established and controlled by the major card issuing brands: Visa, American Express, MasterCard, Discover and JCB. Other firms may also join the Council for a fee, but the founding brands remain firmly in control. The Council exists to promote the Data Security Standards, educate merchants, software developers and the public on data security and oversee the new participants in the process, Approved Scanning Vendors (ASVs) and Qualified Security Assessors (QSAs). Most observers agree that the overarching objective of the card issuers in launching this broad initiative is to protect the consumers' faith in the global payment card system, so that people continue to use their cards to spend, which creates transaction fees for the brands and drives revenues. This level of proactive and aggressive self-regulation by the industry may forestall further legislative regulation intended to protect consumers.

The PCI Security Standards Council owns the PCI Data Security Standards, a group of twelve major requirements that, taken together, define what the card issuing brands define as a secure environment for handling sensitive cardholder data. The major requirements include over 200 specific requirements. Reviewing the specifics of the requirements is beyond the scope of this article, but the AH&LA publication [The Payment Card Industry Compliance Process for Lodging Establishments](http://ahla.com/technology) (see <http://ahla.com/technology>) goes into great detail

on planning and executing the compliance journey for a hotel.

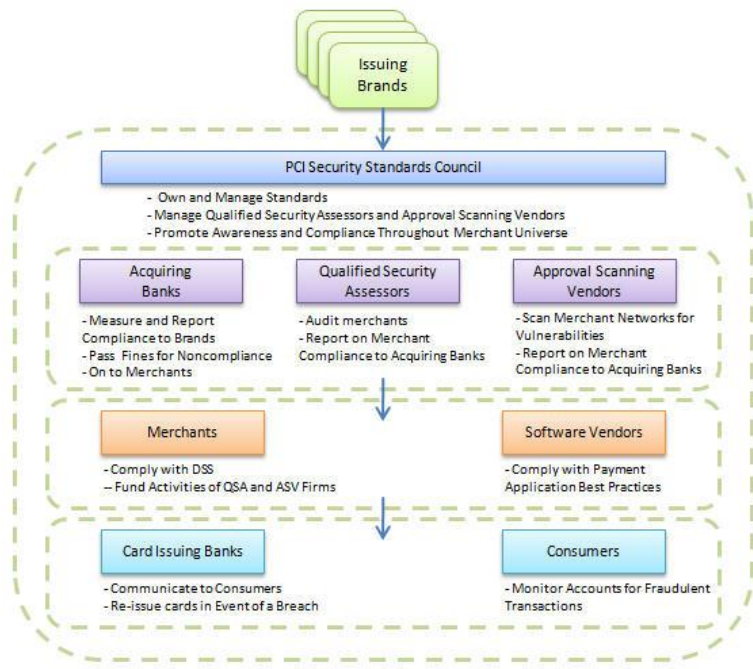
The key things to understand about the PCI Data Security Standards include:

- It is the merchant's responsibility to comply with the standards
- All merchants that accept credit cards, regardless of size, are obligated to comply with all of the standards
- Compliance includes validating full compliance through a self-assessment filed with the merchant's credit card acquirer, usually done with the assistance of a Qualified Security Assessor (QSA)
- Although the standards are owned by the PCI Security Standards Council, enforcement of the standards is done exclusively by the brands
- The brands enforce compliance by fining acquirers, who then pass the fines on to the offending merchant

Many hotel companies of all sizes have been working towards, some even achieving, compliance for a number of years. Some of these companies were surprised by the release in October of last year of version 1.2 of the standards. On the surface, most of the changes in version 1.2 appear to be clarifications, and in some cases simplifications. The SSC also consolidated the standard and the test for compliance into a single document.

However, some of the modifications will have a substantial impact on some hotel companies. Hotel enterprises running large-scale Wide Area Networks (primarily for CRS communications) will find some challenges in segmenting and segregating network

traffic to protect communications with cardholder data. Hotels utilizing wireless networks to carry cardholder data may need to upgrade the encryption protocol in use.



More important than the changes themselves, hotel companies that have begun their compliance initiatives in earnest should continue it. With the exception of the large hoteliers, many hotel companies have not yet begun a meaningful compliance effort.

They have simply ignored it, or assumed that is was someone else's responsibility. Chris Zoladz, Vice President – Information Protection and Privacy for Marriott International, observes "Some franchisees assume that a franchisor handles it all for them. While there may be some dependence on the franchisor for compliance of systems that the franchises uses but the franchisor controls, learning that they are responsible for the compliance of everything else becomes an awakening for them."

Likewise, hoteliers cannot assume that system vendors will make them compliant because they sold them a system with a credit card processing module. As Zoladz stated above, the merchant is solely responsible for compliance. The vendor is not. For a number of years, Visa has administered a program called Payment Application Best Practices (PABP), which certified Payment Applications (such as a Property Management System, Central Reservations System or Point of Sale system) as complying with the Data Security Standards, if installed and maintained by the merchant according to the DSS and the vendor's standards. More recently, this certification responsibility has been transitioned to the Security Standards Council and renamed Payment Application Data Security Standards, or PA-DSS.

For a software vendor to earn PA-DSS certification, they must engage a Qualified Security Assessor (QSA) certified by the SSC to audit Payment Applications. The QSA will examine the programming code and database to ensure that prohibited information (full track data) is not stored, and that card numbers are encrypted in the database and not displayed on screens and in reports, among other DSS requirements. All software applications that process credit card numbers and are sold or licensed to third parties are subject to certification, and must be re-certified annually.

As with the overall PCI DSS, the PA-DSS standards are owned by the Security Standards Council, but enforced by the issuing brands. Visa has published a five phase compliance cycle:

Note Phase V, which requires the acquirers to ensure that all merchants and agents use only PA-DSS compliant applications. The compliance mandate does not specifically require certification, but the burden of proving compliance then falls on the merchant and acquirer. For a hotel company, this means that every PMS and POS installed today must be certified as compliant, otherwise proven compliant by the merchant to the satisfaction of the acquirer, replaced prior to July 1, 2010, or cease processing credit cards, at least Visa.

The costs and managerial implications of this mandate are substantial, especially for larger organizations with potentially many third-party systems to ensure they meet the standard or replaced. Marriott's Zoladz wryly describes the impact as "not trivial" to hotel companies, and goes on to say "The intentions here are good, but seem to lead to unintended consequences for merchants. The costs for operators can be extremely high on a relative scale, especially considering the forced replacement of what is an otherwise effective system with a long usable life remaining, or the burden of ensuring that an not-certified product otherwise satisfies the PCI DSS requirements." The cost impact is obviously heightened in the current economy and the consequent reduction in travel and hotel operating performance.

While some hotel companies may be able to work with their QSA to minimize the number of wholesale system replacements, a lot of hotel companies will be buying a lot of PMS, POS and other applications in 2010. The opportunity presented by PA-DSS has not been missed by most vendors in the space. Many vendors of PMS, POS and CRS systems have completed certification and may be found listed at https://pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html, the official site for certified payment applications.

Investing in PA-DSS certification costs the vendors time and money, and diverts resources from other improvements to their applications and organizations. Vendors of multiple products will

Phase	Compliance Mandate	Effective Date
I	Newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that are known vulnerable payment applications	1/1/2008
II	VNPs and agents must only certify new payment applications to their platforms that are PA-DSS-compliant	7/1/2008
III	Newly boarded Level 3 and 4 merchants must be PCI DSS compliant or use PA-DSS-compliant applications*	10/1/2008
IV	VNPs and agents must decertify all vulnerable payment applications**	10/1/2009
V	Acquirers must ensure their merchants, VNPs and agents use only PA-DSS compliant applications	7/1/2010

* In-house use only developed applications & stand-alone POS hardware terminals are not applicable
 ** VisaNet Processors (VNPs) and agents must decertify vulnerable payment applications within 12 months of identification
 Source: http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html

typically invest in compliance for only one product

each in a major line, rather than pursuing certification for several PMS products, for example. This leads to end-of-life for some systems and a requirement to convert to something else for their installed base of hotels.

Adding up the impact of the new version of the standards and scheduled enforcement of Payment Application enforcement, what does the hotelier do? Simply put, the best advice is to continue on the compliance journey:

- Appoint someone in your organization responsible for compliance
- Give them time, resources and a budget appropriate to the size of the organization
- Utilize the resources of your parent company, franchisor and your acquirer
- Conduct an initial assessment, including:
 - Inventory of all locations where cardholder data is stored, on paper or electronically
 - Certification status of all computer systems in use that capture cardholder data
 - A first pass through the PCI DSS Self-Assessment Questionnaire

- Engage a QSA if necessary to work with you on the Self-Assessment Questionnaire for submission
- Consider PCI compliance an on-going process to be conducted continuously, and expect another version of the standards in 2010

Additional Sources of Information:

The PCI Security Standards Council, <https://pcisecuritystandards.org/index.shtml>. This site offers the Standards themselves and numerous other useful documents supporting the compliance journey.

The American Hotel & Lodging Association, <http://www.ahla.com/technology>. The AH&LA Technology & E-Business Committee publishes two useful resources with rich content specific to hotels: *The Payment Card Industry Compliance Process for Lodging Establishments* and *Principles of Privacy*. Both are available to download, free to AH&LA members or for a nominal fee for non-members.

Visa, the card issuing brand. http://usa.visa.com/merchants/risk_management/cisp.html?ep=v_sym_cisp. Visa has been probably at the leading edge of defining compliance and driving the merchant community to accept it. ■

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 – Lodging Magazine