

Technology: Security

Credit Card Security: Primer on PCI Compliance

By Bob Carr, Chairman & CEO, Heartland Payment Systems



Mr. Carr

If you're not properly securing your guests' sensitive credit and debit card account information, your hotel may be a prime target for the many cyber-criminals who are searching for this valuable data. Data breaches are occurring at an alarming rate as hackers become increasingly sophisticated, constantly finding new and different ways to penetrate electronic systems. Help keep your hotel... and guests... secure by understanding the threats to card data security, the requirements for Payment Card Industry (PCI) compliance and how to meet them.

Threats to Card Data Security

Cardholder data is a major point of vulnerability. Whenever a guest provides a credit or debit card to pay a room balance or for any of your other services, the cardholder's name, card number, card expiration date and security codes may be at risk as they travel from your system, to and through your processor's network. Hotels are particularly vulnerable to data security breaches due to use of point-of-sale (POS) systems, shared systems among chains, wireless networks and the high volume of card-based payments.

If your hotel's data is compromised, private information — stored in your property management or other systems — may be illegally accessed and could lead to theft of card data and other sensitive information, fraud and financial loss. You could face forensic investigations, damage to your reputation, the loss of loyal guests — and stiff fines from the card brands, ranging from tens of thousands to hundreds of thousands of dollars.

As a safeguard, the card brands — Visa®, MasterCard®, American Express® and Discover® Network — developed the PCI Data Security Standards (DSS) in December 2004. These are technical and operational requirements designed to protect cardholder data. Every hotel that accepts card payments — and stores, processes or transmits payment card data — must meet the PCI DSS.

Requirements of PCI Compliance

The PCI DSS include 12 requirements that support six core principles of network architecture, cardholder protection, vulnerability management, access controls, network security and information security policies. This means compliance goes beyond card processing at the point of sale. You must also look at your network and firewall configurations, policies for storing receipts, employees who have access to data, password policies ... and so forth. Here are the PCI DSS principles and corresponding requirements:

- **Build and Maintain a Secure Network**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

- **Protect Cardholder Data**

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

- **Maintain a Vulnerability Management Program**

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

- **Implement Strong Access Control Measures**

Requirement 7: Restrict access to cardholder data by business need-to-know.

Requirement 8: Assign a unique ID to each person with computer access.

Requirement 9: Restrict physical data access to cardholder data.

- **Regularly Monitor and Test Networks**

Requirement 10: Track and monitor all access to network resources and cardholder data.

Requirement 11: Regularly test security systems and processes.

- **Maintain an Information Security Policy**

Requirement 12: Maintain a policy that addresses information security.

It is important to understand these requirements for the overall safety of your establishment and your guests. And this is particularly timely because, since July 1, 2010, Visa's security mandate has required merchants to use a PCI-compliant payment application. This means you cannot use an application that stores prohibited data elements, such as magnetic stripe data.

Meeting PCI requirements is an important step, but being compliant is not easy. Beyond the 12 requirements, there are more than 230 PCI regulations you may have to meet depending on your processing environment. Plus, the self-assessment questionnaires (SAQs) that validate compliance can be tedious and time-consuming to complete.

PCI Compliance Tips

To alleviate some of the confusion surrounding PCI compliance, there are several steps you can take. Follow these best practice tips to ensure PCI compliance at your hotel:

- Meet all PCI DSS requirements. Using a validated payment application may help improve PCI compliance. However, to be considered PCI DSS-compliant,

you need to validate your compliance. For most merchant levels, determined by transaction processing volume, you can do that by completing the SAQ and passing network vulnerability scans (detailed below). If additional validation is required, your processor should notify you.

- Complete the PCI DSS SAQ to identify any vulnerabilities at your hotel. There are four versions of the SAQ — each version with a different number of questions depending on the business's processing environment. A business processing card payments via a phone dial-up connection will have fewer questions to answer than a business processing via an internet connection since the internet connection offers an external portal. Use a Qualified Security Assessor (QSA) to help with your PCI SAQ, and consult your network support person and/or property management or other system software provider for assistance with questions about your set-up and environment. To be compliant, your hotel must complete and pass the SAQ annually. If you process payment cards using multiple computers, you only need to complete one SAQ.
- Complete a network vulnerability scan if you have an external-facing IP address. An external probe of all of your IP addresses will help identify any of more than 30,000 — and counting — commonly known vulnerabilities hackers exploit. In 2009, more than 8,000 new vulnerabilities were discovered, which averages out to almost 20 each day.

To complete a network vulnerability scan, work with an Approved Scanning Vendor (ASV) listed on the PCI Security Standard website, PCISecurityStandards.org, under "QSA/ASV." To be compliant, your hotel must complete and pass the network vulnerability scan quarterly.

- Complete additional system reviews as needed. If you use a POS or other networked system, you may be storing cardholder data. Some services are available that can search your system to determine this. If the payment card data search detects track data, you should contact your software system provider immediately to upgrade your payment application and ensure they securely remove all prior-stored, prohibited data. This is essential to ensure compliance with this requirement of the PCI DSS and reduce your exposure to compromise.
- Consult your payments processor. Ask your payments processor for more information and help in ensuring your hotel is PCI compliant.

Full information about PCI and the necessary forms are available on the PCI Security Standards Council website, PCISecurityStandards.org.

Bob Carr is chairman and CEO of Heartland Payment Systems. Mr. Carr co-founded Heartland in 1997, and took the company public in 2005. Heartland has 150,000 customers and 2,250 employees - and increased its portfolio to almost \$55 billion. Mr. Carr has written articles to educate merchants on the acquiring industry. He spearheaded "The Merchant Bill of Rights" to promote fair credit and debit card processing practices for all business owners. Mr. Carr holds a B.S. and M.S. in mathematics and computer science from the University of Illinois. Mr. Carr can be contacted at Bob.Carr@e-hps.com

Hotel Business Review

Best practices in hotel management and operations...

The Hotel Business Review is a weekly journal of best practices in hotel management and operations and is available at www.hotelexecutive.com. HotelExecutive.com retains the copyright to the articles published in the Hotel Business Review.

Articles cannot be republished without prior written consent by HotelExecutive.com.