

# MerchantResource



## The Payment Card Industry Data Security Standard: Tips and Tricks

### Most Common Data Security Flaws

Data compromise investigators find that hackers, more often than not, breach a payment card environment by exploiting one or more of these basic weaknesses within a system's network:

- Lack of or miss-configured firewall
- Out of date patches
- Lack of or expired anti-virus software
- Easy passwords

While addressing these vulnerabilities will not make an organization PCI DSS compliant, implementing solutions are the first steps to achieving compliance.

### Firewalls

In today's connected world, system firewalls are a necessity. A firewall is an organization's first defense against network intrusion. A network without a firewall welcomes hackers.

Implement a firewall device for your network. PCI DSS also requires the installation of a separate firewall in front of any system that contains any cardholder data.

During configuration, confirm that:

- A rule is set to deny all inbound and outbound network traffic not relevant to the business.
- The firewall is set to use Network Address Translation (NAT) to disguise internal addresses.
- The firewall uses stateful inspection.

### Don't Risk it ... Get Compliant.

To help its merchants achieve PCI DSS compliance, Chase Paymentech partnered with AmbironTrustWave, a compliance management and data security expert, to provide the expertise you need to get compliant. AmbironTrustWave works with thousands of merchants, from mom-and-pop shops to global operations, guiding them through the PCI DSS compliance process.

AmbironTrustWave's TrustKeeper® is an easy-to-use Web portal that helps merchants complete the PCI DSS Self-Assessment Questionnaire, schedule required scans, manage onsite audits and answer the questions they have about their network environment and PCI DSS compliance.

To get started, visit

<http://www.chasepaymentech.trustkeeper.net>

If you have any questions, please contact AmbironTrustWave support at 1-888-878-7817.

## Patching

Vendors often release updates, or patches, to their software to repair problems and address vulnerabilities in an application's source code. Hackers then write programs to exploit these vulnerabilities and gain unauthorized access to a network. Because these exploits can spread rapidly, patch management is an integral part of any security program.

Your organization should do the following to keep all systems and applications up-to-date:

- Contact vendors to ensure you're using current versions of their software.
- Take advantage of your application's automated update features.
- Ensure that patches are installed as soon as possible upon release.

## Anti-virus

A virus attached to an e-mail gives hackers just what they need to compromise a network. Organizations should use anti-virus software to identify and eliminate malicious software.

Follow these steps to protect your network from malicious code:

- Choose anti-virus software that can also detect and delete spyware and ad-ware.
- Install the software on all work stations and servers.
- Take advantage of automatic update features.
- Keep your subscription current.

## Passwords

Institute and enforce a password policy that requires passwords be unique and not easily identifiable. Your policy should apply to all users, guests, people who connect remotely and even applications that have their own built-in passwords. Within your password policy, specify that:

- Vendor default passwords may not be used.
- Passwords must include uppercase and lowercase letters, numbers and special characters.
- Passwords must be changed at least every 90 days.

## Remember...

Incorporating this information into your data security policy alone will not make you PCI DSS compliant. These tips only cover some critical basics that can help you work toward compliance.

Another basic step to take toward achieving PCI compliance is making sure you're application adheres to Visa's Payment Application Best Practices (PABP). The majority of payment card compromises can be blamed on weak payment applications. To see a list of PABP-validated payment applications, please visit Visa's Web site. Confirm that your payment application's release and version number both appear on the list.