



May 17 2010 - Industry News

Are You PCI Compliant Yet? 12 Ways To Know For Sure

Crystal Sulzer of Ferrari Merchants reviews 12 essential requirements for operators to check and verify before they can be considered PCI compliant.

A PCI compliance deadline for the credit card processing industry is just around the corner. By July 2010 all merchants must be certified that they are compliant with the Payment Card Industry Data Security Standards. With more and more diversity on how we take credit cards, it has become more confusing to the merchant as to whether PCI applies to them or not. PCI APPLIES TO EVERYONE; even the companies that take only one or two cards a year.

There are 12 requirements that a merchant must follow and adhere to when dealing with customers' credit card information.

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

a. By installing a firewall, this helps minimize the exposure from people trying to hack into your system. There is not guarantee that someone cannot hack a firewall; but it does help minimize the accessibility of your system from people just randomly surfing systems.

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

a. Again, some of this is common sense. Use a password only you are going to know. Keep a list of your password accessible for your eyes only. Some systems will even tell you how secure your password is.

3) Protect stored data.

a. Do not store cardholder data unless it is really necessary.

b. Do not email sensitive information such as full card number and expiration dates.

c. Do not locate servers or other payment card system storage devices outside of a locked, fully secured and access-controlled room.

d. Once information is stored, you should not have the full account number or the expiration date accessible at all.

4) Encrypt transmissions of cardholder data across open, public networks

- a. Again, the full credit card number should never be seen.
 - b. If you are working on a system that has multiple users, make sure they only see the data on a need to know basis and only have access if absolutely necessary.
- 5) Use and regularly update anti-virus software
- a. Virus software doesn't also help protect your data, it also helps protect your e:mails. Viruses can attach them selves to e:mails and kill you computer.
 - b. Recommendation is not to use just free anti-virus software. Remember you get what you pay for.
- 6.) Develop and maintain secure systems and application.
- a. Know what software you are putting on your system. Downloading applications from the internet can have spy ware leaving your computer compromised even if you have a firewall, because you gave it permission to be on your system.
- 7) Restrict access to cardholder data by business need to know.
- a. Not every person in your company needs to know the billing information of your clients. Passwords restrict those who don't need to know.
- 8) Assign a unique ID to each person with computer access.
- a. By assigning unique ID's, if a compromise does happen it's easier to trace who actually accessed information that they didn't need.
- 9) Restrict physical access to cardholder data.
- a. If you are storing actual receipts, make sure they are in a secure location under lock and key, filed and secured with limited access to only key personnel.
- 10) Track and monitor all access to network resources and cardholder data.
- a. Simply test your networks to make sure there is no breaches
- 11) Regularly test security systems and processes
- a. Have some type of policies and procedures in place to assure when employees leave, they no longer have access to secure data.
 - b. There are SAQ's (Self Assessment Questionnaires) available to help in these areas.
- 12) Maintain a policy that addresses information security.
- a. Again have procedures in place to address the employees need to know basis.

Just because you believe you've completed the above does not make you compliant. This is a continual process and must be done once a year to ensure the best possible safety for the cardholder data that you store. One company does not make you compliant, because as you can see, there are many moving parts. If the engine breaks down, the whole car doesn't run. It's the same here. Look at the big picture of processing; you as a consumer want to make sure your data is protected by companies you're dealing with, it's the same for you're clients.

I always recommend to make sure you have an IT company that can help you in the above areas that you may not be comfortable on, or may not know about. Using the everyday Router with firewall for your home is not as secure as a company that specializes in these types of security for major networks.

PCI may seem overwhelming, but it really comes down to good security, good practices, and good employees. PCI may not be cheap, but in the long run, it can save you.

Crystal Sulzer is the managing partner of Ferrari Merchants in Tomball, Texas.

[PREVIOUS FERRARI MERCHANTS F&I ARTICLE HERE.](#)

Tags: Credit Card Compliance, Credit Card Processing, Ferrari Merchants

[Request more info about this product / service / company](#)

© Copyright 2010 LCT Magazine. All Rights Reserved.