

New Credit Card Security Standards FAQ

Who is required to meet the PCI security standard?

All entities that accept credit or debit card payment, collect, process or store credit card transaction information, regardless of their transaction volume, are required to meet the PCI standard by June 30, 2005. Failure to comply with the PCI security standard may result in substantial fines or permanent expulsion from card acceptance programs.

All Acquiring Banks (merchant banks) are also required to have received certified proof of PCI compliance from merchants with more than 20,000 transactions per year by June 30, 2005. This does not mean that only merchants with more than 20,000 transactions per year are required to meet the PCI standard. Acquiring Banks are required to have documented proof of compliance from these merchants, or be liable to fines themselves. Many banks are already requiring all merchants, regardless of transaction volume, to produce this Certification of PCI Compliance.

What are the PCI security standards?

The new Payment Card Industry (PCI) data security standards are network security and business practice guidelines developed by Visa, MasterCard, American Express and Discover Card. They were developed to establish a 'minimum security standard' with regards to the protection of cardholders' account and transaction information.

What do I need to do to meet the PCI standards?

The PCI standard comprises two basic steps:

1. Pass quarterly remote vulnerability scans conducted by an a Visa and MasterCard "Qualified Independent Scan Vendor" such as ScanAlert Inc. Scans are required for all Internet connection points whether they are office networks or home/office connections (dial-up, DSL, cable or wireless) or permanent Internet servers such as your web site and email server, etc.
 2. Successful completion of a security self-assessment questionnaire. The self assessment questionnaire asks specific questions about your internal security practices, both on your web site and in your office. ScanAlert provides an online "wizard" tool to help you properly complete this form.
-

What does ScanAlert's Certified PCI Compliance service include?

ScanAlert's comprehensive and easy-to-use PCI certification service includes:

- Access to ScanAlert's web-based Vulnerability Management Portal
- Scheduled quarterly automated vulnerability scans
- Unlimited on-demand manual scans to re-test systems whenever needed
- Detailed instructions to patch all vulnerabilities found during scans
- Online tutorials to help understand and prepare the security self-assessment questionnaire
- Preparation of the Report on Compliance (ROC) documentation for submission to your

- merchant bank
 - Access for your merchant bank to review your Report on Compliance online
-

Who is ScanAlert?

ScanAlert is the world's largest ecommerce security auditing company, protecting and certifying more than 70,000 web sites in 71 countries through its HACKER SAFE trustmark program. ScanAlert is accredited by MasterCard and VISA to provide PCI compliance services. More information is available at <http://www.ScanAlert.com>

As a Visa and MasterCard "Qualified Independent Scan Vendor," all credit card companies and banks worldwide accept ScanAlert's Certification of PCI Compliance.

If ScanAlert is going to prepare my company's Visa PCI Compliance Report, why isn't ScanAlert on the Visa CISP Assessor List?

Only merchants with over 6 million transactions per year require an on-site audit, conducted by a "Qualified Independent Security Assessor, or Visa CISP Assessor," in addition to network scans conducted by a "Qualified Independent Scan Vendor" such as ScanAlert.

For merchants transacting more than 6 million credit card purchases per year, and all levels of payment processors, ScanAlert will provide a quote for an on-site CISP Level 1 Compliance Assessment performed by our CISP Assessor partner, PSC.

What if the scan result shows that my site has vulnerabilities?

Complete instructions for patching any vulnerabilities are available within your Vulnerability Management Portal. This information can be easily made available directly to your web host or IT staff using your ScanAlert account. Online technical support is also available.

What do I do after my web site has been scanned and I have completed the security self assessment?

Within your Vulnerability Management Portal, you can print a PCI compliance report as well as the completed self-assessment form. You may also have ScanAlert submit this information directly to your merchant bank.

Does ScanAlert provide customer support as part of its PCI data security service?

Customer support is available through ScanAlert's online portal where you will find a variety of resources, including interactive tutorials, best practices information, FAQs and online support request forms to help you understand how to pass the security scans as well as complete the self- assessment questionnaire.

What if I have already paid for compliance from another PCI security company?

If you are already using another PCI security scanning service, you can easily switch to ScanAlert and save hundreds or thousands of dollars. All credit card companies and all banks accept ScanAlert's Certified PCI Compliance.

Where can I get more information about meeting the PCI standards?

More information, including complete step-by-step instructions for meeting the PCI requirements are available within your ScanAlert account under the PCI tab.

Where can I find references about the PCI requirements?

PCI program summary:

https://sdp.mastercardintl.com/pdf/pcd_manual.pdf

PCI security scanning procedures:

https://sdp.mastercardintl.com/pdf/PCS_Manual.pdf

PCI self-assessment questionnaire:

https://sdp.mastercardintl.com/pdf/758_PCI_Self_Assmnt_Qust.pdf

Merchant definition matrix is available at:

https://sdp.mastercardintl.com/merchants/merchant_levels.shtml