

Staying Compliant with VISA, MC, American Express...

Increased Credit Card Fraud Causes Change

In recent years, credit card fraud has become more than just an embarrassment to companies like Visa, MasterCard and American Express, it has become a threat to their survival. The days of the lone hacker are over. Now, highly-skilled and organized thieves not only plunder the coffers of big business, they are threatening to undermine

the entire system by eroding the confidence of the consumer.

And the major credit card companies have realized they cannot control the situation alone. They can no longer support the legacy model of reimbursing the merchant for fraudulent charges without the commitment from the merchant to do everything they can to ensure the security of online transactions.

The Payment Card Industry Data Security Standard

In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International announced the formation of the PCI Security Standards Council (PCISSC). The goal of the council is to ensure that merchants and service providers who send data electronically, have taken steps to protect transactions. These requirements apply

to all payment card network members, merchants and service providers that store, process or transmit cardholder data, and affect all payment channels, including retail (brick-and-mortar), mail/telephone order and e-commerce.

These requirements are imposed by the PCISSC, not by any government agency. **Meeting the requirements of the Council is now a prerequisite to doing business with the major credit card companies.** You don't have to meet these standards—but you may not be able to process credit cards either.

The core requirements of the PCISSC are:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

While these requirements may appear daunting, Quest can perform scanning that will help identify any shortcomings or non-compliance problems that may exist in your systems. These scans can be performed remotely or on premises. And the cost for this type of scanning is surprisingly low.

Companies that do not meet the PCISSC's requirements may be barred from processing credit cards, incur higher processing fees and even face fines up to \$500,000.

Quest is a PCI Security Standards Council Approved Scanning Vendor.

PCI SSC Scanning Vendor (Compliance Certificate Number: 3845-01-07)



Contact Quest
800.326.4220 | www.questsys.com



Validation Compliance

All merchants and service providers, regardless of credit card transaction volume and acceptance channel, must fulfill two validation requirements. Some merchants and service providers validate compliance through an Annual On-Site Security Audit and Quarterly Network Scan, while others complete an Annual Self-Assessment Questionnaire and Quarterly Network Scan. Compliance levels for merchants and service providers are defined based on annual transaction volume and corresponding risk exposure.



Compliance levels are defined based on annual transaction volume and corresponding risk exposure as outlined in the figure below:

| | Level | Criteria | On-Site Security Audit | Self-Assessment Questionnaire | Network Scan |
|-------------------------|-------|--|------------------------|-------------------------------|--------------------|
| Merchant | 1 | <ul style="list-style-type: none"> Any merchant, regardless of acceptance channel, processing more than 6 million transactions per year Any merchant that suffered a security breach, resulting in an account compromise | Required Annually | | Required Quarterly |
| | 2 | <ul style="list-style-type: none"> Any merchant processing between 150,000 to 6 million transactions per year | | Required Annually | Required Quarterly |
| | 3 | <ul style="list-style-type: none"> Any merchant processing between 20,000 to 150,000 transactions per year | | Required Annually | Required Quarterly |
| | 4 | <ul style="list-style-type: none"> All other merchants not in levels 1, 2, or 3, regardless of acceptance channel | | Required Annually | Required Quarterly |
| Service Provider | 1 | <ul style="list-style-type: none"> All processors and all payment gateways | Required Annually | | Required Quarterly |
| | 2 | <ul style="list-style-type: none"> Any service provider that is not in Level 1 and stores, processes or transmits more than 1 million accounts/transactions annually | Required Annually | | Required Quarterly |
| | 3 | <ul style="list-style-type: none"> Any service provider that is not in Level 1 and stores, processes or transmits less than 1 million accounts/transactions annually | | Required Annually | Required Quarterly |

Quest’s “Compliance Vulnerability Scanning” Professional and Managed Services are PCI SSC Scanning Vendor Compliance (Certificate Number: 3845-01-07)

Contact Quest
800.326.4220 | www.questsys.com

The PCI Security Standards Council log is a trademark of PCI Security Standards Council, LLC.

