



A PCI Compliance Primer



Introduction

With the mission of protecting and securing credit card data, the Payment Card Industry (PCI) Security Standards Council has established specific compliance requirements for companies that process, transmit or store credit information. Companies are classified as either merchants or service providers (service providers are entities that perform a function such as processing a credit card transaction or providing backup tape storage of credit card data).

The quantity of credit card numbers handled on an annual basis determines the categorization level of merchants and service providers. For example, Level 1 merchants and Level 1 and 2 service providers are required to conduct annual, on-site assessments that can only be performed by a **Qualified Security Assessor (QSA)** such as Accudata Systems, Inc. Merchant and service providers that handle lower numbers of credit cards are required to complete a PCI self-assessment questionnaire (an on-site QSA audit is not required).

To assist with the compliance effort, many organizations seek the knowledge and experience of a QSA to help them prepare for an upcoming audit, assist with the completion of a self-assessment questionnaire, and obtain clarification on the required PCI Data Security Standard (DSS) controls. Figure 1 (next page) defines PCI's four merchant levels, the required validation actions, who must perform the validation, and the date the validation is due. Figure 2 (next page) illustrates the process that Accudata Systems follows for a PCI engagement.

Accudata Systems PCI Services

As an approved QSA with experienced PCI consultants, Accudata Systems is qualified to provide clients with:

- Annual on-site PCI DSS assessments
- Pre-PCI audits and remediation services
- Assistance with the completion of the Self-assessment Questionnaire
- Consultation on payment processes and architectural design

Penalties

Noncompliance with the PCI Data Security Standards can result in fines and higher processing fees. Firms found to be storing extremely sensitive credit card data (e.g., PINS, full magnetic stripe track data, or card verification value CVV2 data) can be subjected to monthly fines of \$10,000. For example, in 2006 Visa indicated that they levied \$4.6 million in fines versus only \$3.4 million in 2005. Accudata Systems consultants have seen fines ranging from nominal to \$500,000 for the improper handling of credit card track data.

Achieving Compliance

The most commonly experienced roadblocks to PCI compliance center around the following four topics: (1) Data encryption, (2) Access management, (3) Application security, and (4) Logging. According to a Gartner study quoted in the 10/2/2007 edition of the Wall Street Journal, the cost of achieving compliance can be significant. The table below shows the average dollar amounts that merchants spend on new technology to comply with PCI requirements (does not include service costs).

Merchant Level	Average Technology Investment
Level 1 Merchant	\$568,000
Level 2 Merchant	\$267,000
Level 3 Merchant	\$ 81,000

Given the roadblocks, technology expenses, potential fines and maze of requirements facing merchants and service providers, it is both cost effective and expedient to consult with an experienced QSA at the beginning of the process to maximize your investment and protect your PCI data.

For More Information

To find out more about our PCI Compliance services, please contact Accudata Systems at 800-246-4908.

Figure 1. Merchant Levels Defined by Visa

Merchant Level*	Description
1	Any merchant, regardless of acceptance channel, processing over 6,000,000 transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize the risk to the Visa system.
2	Any merchant, regardless of acceptance channel, processing 1,000,000 to 6,000,000 Visa transactions per year.
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants, regardless of acceptance channel, processing up to 1,000,000 Visa transactions per year.

* New merchant level definitions effective as of July 18, 2006.

* Any merchant that has suffered a hack that resulted in an account data compromise may be escalated to a higher validation level.

* From www.visa.com/merchants/risk_management (October 2007).

Figure 2. Accudata Systems PCI Process Flow

