



PAI Secure Program Guide



A complete guide to understanding the Payment Card Industry Data Security Requirements and utilizing the PAI Secure Program.



Letter From the CEO

Welcome to PAI Secure.

As you should now be aware, all U.S. merchants accepting credit and debit cards have been mandated to meet a series of requirements relating to data security.

These requirements have been issued by the Payment Card Industry Data Security Standards Council, the governing body comprised of all the primary card companies including Visa, MasterCard, American Express and Discover.

The complexity and evolving nature of these standards has left all of us struggling to get a clear definition of the rules and feeling a little overwhelmed by the many requirements. The bottom line is that we all had new industry requirements that we had to comply with as of October 1, 2008. Failure to comply with these standards may result in significant fines being assessed by the card associations against your business and you may be subject to potential losses as a result of your non-compliance with these new PCI standards.

It is important to recognize that PCI exposure is not limited to e-commerce merchants or only those merchants transacting business where the physical card isn't present. PCI applies to ALL merchants and many losses occur simply because the business held card data too long or wrote down a number for later authorization. Standard business practices must be re-evaluated and protective measures implemented.

As your payment processing partner, Payment Alliance International (PAI) developed a comprehensive program designed to facilitate your total compliance and guide you through these changes. Our goal is to keep you and your business safe and to provide protection against unforeseen business exposures.

PAI Secure goes far beyond simply "making you aware". This program walks you through the compliance process and mitigates the risks to your business by providing you with educational programs, assistance with completion of the required "Self-Assessment Questionnaire", a PCI risk management website, a PCI Hotline staffed with knowledgeable Compliance Agents, and PAI PCI Indemnification Coverage for up to \$100,000.00 protection for documented and qualified losses for an Umbrella of Protection.

This PAI Secure Program Guide will get you started by giving you a summary of requirements along with the instructions you need to implement and maintain this program. Inside this helpful booklet you will find an overview of the PAI Secure program, including an introduction to our online PAI Customer Information Center. Everything you need to help you understand the PCI rules and our industry's "get tough" policy can be found here.

At Payment Alliance International, success has always been measured by the results we deliver for the clients we serve. We will continue to work hard to make PCI compliance as easy as possible. PAI Secure Compliance Agents are standing by to assist you with any questions you may have, so please call us at 866-275-5922 or email us at PAIsecure@GoPAI.com

We appreciate your business and are grateful that you've chosen PAI as your payment processing partner!

Sincerely,

John J. Leehy, III
President & CEO
Payment Alliance International, Inc.

Payment Card Industry (PCI) Data Security Standard (DSS)

What is the Payment Card Industry Data Security Standard (PCI DSS) and how will it affect your business?

In December 2004, Visa and MasterCard (later joined by American Express, Discover and JCB) announced the creation of the PCI DSS Council, whose mission was to design rules and regulations aimed at reducing the loss of proprietary cardholder data occurring at merchant locations accepting these brands. The resulting programs required that ALL businesses meet new and more stringent security standards by October 1, 2008. Additionally, this governing body has instituted a framework of fines and penalties for both the failure to comply with these requirements as well as ANY loss of cardholder data. Fines are already being assessed in conjunction with security breaches.

Please note: Whether your card transactions are processed on a sophisticated Point of Sale system via the Internet or through a traditional stand-alone Point of Sale terminal plugged into a phone line, the rules of PCI DSS apply to you. **According to the PCI Council, any company processing, storing, or transmitting payment card data must be PCI DSS compliant or risk losing their ability to process credit card payments.**

Why does this matter to you?

- 85% of card compromises identified since February 2008 occurred at Level 4 businesses (like so many of our best customers). Source: Visa
- 77% of customers surveyed said they would stop shopping at merchant locations they believed were capable of card data breaches. Source: Javelin Strategy & Research, 2007

How can this happen when your terminal truncates numbers and does not store any cardholder data?

Many breaches happen due to internal employees being careless with the physical card. Thieves can quickly and easily copy sensitive card data without touching your terminal or system.

What must you do to become compliant?

- You must stay up-to-date on all of the compliance regulations.
How: PAI Secure provides you with all of the regulations, makes them easy to understand and helps you realize maximum protection for a minimum of costs.
- You must fill out an annual Self-Assessment Questionnaire.
How: PAI Secure gives you the questionnaire, provides tools to help you complete and submit.
- If your business fits certain criteria, you must submit to a quarterly IP scan.
How: PAI Secure helps you determine if you need a scan and links you to our certified scanning partner so that your scan can be completed.

*"The PCI Security Standards Council is committed to helping everyone involved in the payment chain protect consumer payment data."
Bob Russo,
General Manager
of the PCI
Security
Standards
Payment Card
Industry (PCI)
Data Security
Standard (DSS)
Council*

Payment Card Industry (PCI) Data Security Standard (DSS)

A PCI DSS survey conducted in 2007 by Ambion Trustwave shows that 92% of all data breaches occur with small merchants doing less than 20,000 transactions per year. This statistic challenges the popular belief that thieves target larger businesses because they accept more payment card transactions. Council

Here are 12 key requirements for protecting cardholder data:

- 1. Firewall rules.**

PCI standards require that all systems coming in contact with cardholder data be protected by firewalls if those systems support e-commerce or some other use of the Internet such as e-mail.
- 2. Change system passwords from vendor-supplied defaults.**

These passwords and settings are well-known in "hacker" communities. They need to be changed before you connect to your network.
- 3. If you store it, protect it.**

Unless it's absolutely necessary to retain cardholder data, don't! And if you do, make sure controls are in place which minimize the risk of cardholder information getting into the wrong hands.
- 4. Encrypt all numbers in transit.**

When sending sensitive data (like card numbers) across public networks, encryption is a must. That goes for e-mail too. Unencrypted account numbers should never be sent by e-mail.
- 5. Use anti-virus software.**

As anyone with an active e-mail account can attest, malicious viruses and other attacks can slip through firewalls and end up in your electronic in-basket. Not only do you need anti-virus software, but you must also update it regularly.
- 6. Keep up with security patches.**

PCI standards require all systems that might come into contact with payment card data to have up-to-date software patches that don't run afoul of existing security configurations. In-house developers need to be aware of and take PCI into consideration when creating patches for any of those systems.
- 7. Keep data away from wandering eyes.**

There's very little need for most personnel to see critical cardholder data. For any computing resources using that data, limit access to people whose jobs require access. Systems with multiple users may require special mechanisms that partition access on a need-to-know basis.
- 8. Require and assign unique user ID's.**

Unique ID's ensure that you have a way to know who touches what data and when.
- 9. Keep a tight lock on card data.**

Physical access to cardholder data or the systems that house that data must be monitored and restricted. This includes any paper or electronic media containing cardholder data.
- 10. Keep tabs on everything and everyone.**

Be aware and keep track of anyone who uses your systems or terminals.
- 11. Test everything regularly.**

Systems and controls should be tested at least quarterly and following any upgrades or modifications by vendors qualified in PCI compliance.
- 12. Make security "job one".**

Every organization (including large and small) needs a strong security policy, and the policy should be put into writing. "It sets the security tone for the entire company and informs employees on what is expected of them," states the PCI Security Standards Council.

While these minimum data management standards are mandatory and required of all card accepting merchant locations, simply fulfilling these requirements WILL NOT fully protect you from all fines and losses resulting from theft or loss of cardholder data (data breach). However, it is required that all businesses be able to evidence their compliance with these twelve basic safeguards.

Payment Card Industry (PCI) Data Security Standard (DSS)

The requirement for evidencing full compliance is determined by the category that your business falls into (outlined on chart below):

Merchant Criteria	Validation Requirements
Level 1 Merchants processing over 6 million transactions annually (all channels) or global merchants identified as Level 1	*Annual Report on Compliance (ROC) by Qualified Security Assessor (QSA) *Quarterly network scan by Approved Scan Vendor (ASV) *Attestation of Compliance Form
Level 2 Merchants processing 1 million to 6 million transactions annually (all channels)	*Annual Self Assessment Questionnaire (SAQ) *Quarterly network scan by ASV *Attestation of Compliance Form
Level 3 Merchants processing 20,000 to 1 million (any channel) e-commerce transactions annually	*Annual SAQ *Quarterly network scan by ASV *Attestation of Compliance Form
Level 4 Merchants processing less than 20,000 (any channel) e-commerce transactions annually and all other merchants processing up to 1 million (any channel) transactions annually	*Annual SAQ *Quarterly network scan by ASV, if applicable *Compliance validation requirements set by acquirer

"Data security breaches involving payment card information occur at small businesses more frequently than at all other merchant levels combined."
Michael E. Smith,
VisaCouncil

Initially the PCI DSS program was appropriately targeted at **Level One** through **Level Three** merchants since this group represented the largest number of transactions, often had more expansive POS systems and technologies, and included all e-commerce and internet based merchants. *Now ALL merchants must comply with the standards whether your business utilizes a stand-alone terminal connected to a phone line or a more complex POS system transmitting transactions over the Internet.*

Payment Card Industry (PCI) Data Security Standard (DSS)

Means of misuse of stolen card:
41.6% - In-person purchases
16.0% - By phone or mail
23.9% - Online purchases
Source: Javelin Strategy & Research, 2007

The acquiring industry has seen a significant rise in the number of Level 4 merchants becoming victims of breaches of the PCI DSS requirements in the following ways:

1. Theft of computers with POS systems containing cardholder data.
2. Theft of cardholder data by an employee recording cardholder numbers.
3. Theft of cardholder data by a breach of the business' firewall by hackers.
4. Theft of cardholder data from sales receipts by unauthorized personnel.

Many of these situations were identified by the PCI Council following complaints by various cardholders, identifying the businesses at which these cards were used. Despite the fact that there existed no reason to believe the principals were involved, significant fines, penalties and audits are pending against these businesses.

In these cases, the process followed by the card associations (VISA, MasterCard, American Express, Discover and JCB) is listed below.

Common process to uncovering a data breach

Many suspected security breaches are initiated by a cardholder complaint. Here's how the process works:

1) Cardholders complain to their issuers:

Consumers report a possible fraud on their card (not necessarily at your location).

2) Issuers notify the card companies

(Visa, MasterCard, American Express, Discover or JCB):

3) Card companies investigate fraudulent card use

Card companies determine where the card has been used for the last six months.

If used in your location in this time period, you may then have to submit to a forensic audit. This mandatory audit is on-site and conducted only by qualified security assessors.

The cost to you for this can be \$10,000 or more.

4) Forensic audit is performed to determine the cause of the data compromise

The audit report determines if there has been a breach, how it occurred and most importantly if you are PCI DSS compliant.

5) Fines are assessed

Non-compliance is a major determining point whether fines will be imposed. Fines can be as high as \$500,000. The card companies can also require you to pay for the reissuance of compromised cards (\$25 to \$50 a card), as well as any reimbursement for fraud activity. Certain states have enacted laws as well giving the state also has the ability to impose fines on you as well.

Bottom line: you can suffer financial fines, reimbursement fees and audit costs totaling \$25,000 to \$100,000+

PAI Secure: Making Compliance Work



Recognizing the risks posed to all of our customers, PAI has created a program to both help your business comply with the PCI DSS requirements and protect you in cases of a data breach. This program is called PAI Secure.

Why do you need PAI Secure?

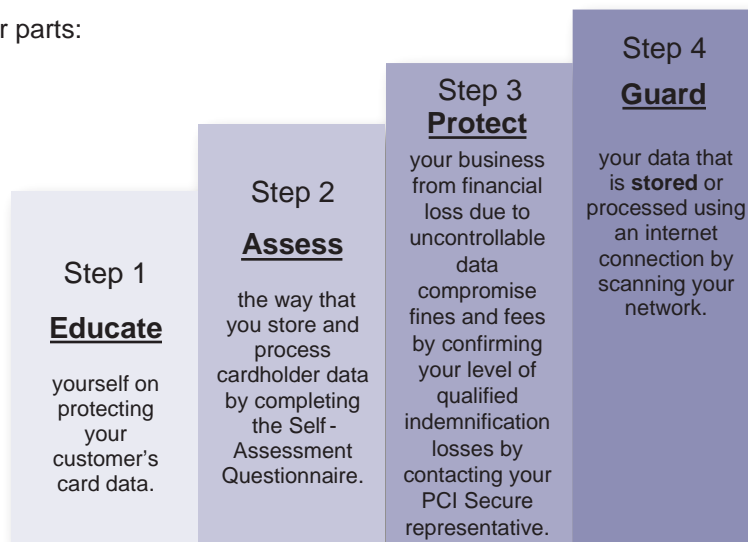
Ask yourself these questions:

1. Are you aware that you are prohibited from storing any cardholder magnetic stripe data and also have requirements for storage of any cardholder information?
2. Do you have a written and communicated policy for data security?
3. Is your equipment PCI compliant? ALL POS manufacturers are now required to get their terminals and applications certified and listed on the PCI Payments Application Data Security Standard (PA-DSS) report
4. Has your system or terminal been identified as "end of life" as a result of the aforementioned PA-DSS report? Effective in 2010 only PABP approved POS applications can accept payments.
5. Does your system store cardholder data without your knowledge?
6. Can you afford a forensic audit costing an average of \$10,000 with resulting fines of \$25,000 or more?

Even if you are comfortable that you have covered all of the above, keeping up with the ever evolving world of PCI DSS is difficult at best. PAI Secure is a one-stop solution for keeping you up-to-date on all of the requirements and providing the resources to maintain compliance.

PAI has created a unique program to assist your business in completing the twelve compliance standards, and protecting your business against the financial consequences of a data breach.

The program consists of four parts:



All four components of the **PAI Secure** program are available online through our web site at www.paicustomerinfo.com. Once on the site, choose the PAI Secure option and begin the compliance process. The site will step you through the process and provide you with useful educational information. You may also call (866) 275-5922 to speak to a representative about the program.

60% of data compromises disclosed by merchants to date have involved outdated versions of third-party software.
Source: Ambiron Trustwave

PAI Secure: Making Compliance Work

To access all steps outlined below please follow these instructions:

1. Go to www.PAICustomerInfo.com
2. Click on the PAI Secure button
3. The buttons will indicate each step. Click on the appropriate button to initiate that step.

Step 1 - Education

This module provides updated compliance mandates and dates. Selecting this option provides key compliance information, statistics on compromises/losses and valuable links to industry information. Templates assist in developing internal data security policies, training videos for educating employees and access to POS upgrades that are available.

Step 2 - Self-Assessment Questionnaire (SAQ)

Mandatory Requirement of PCI for ALL Merchants Regardless of Volume and Technology

The SAQ is a set of questions designed to evaluate business security practices. Successful completion of the questions identify potential business vulnerabilities regarding cardholder data.

By selecting this option you will answer a simple set of questions (no more than five) to determine which form of the SAQ will apply to your business, a link to the applicable form and instructions on how to print, complete and submit the SAQ.

If assistance is required, contact our PAI Compliance Experts or purchase access to an additional level of online support that will provide the ability to complete the form online, submit the form real time and warehouse a copy for retrieval any time.

Step 3 - PAI Secure Merchant Compromised Data Expense Reimbursement Indemnification Coverage Program

The PAI PCI Secure Indemnification Coverage helps businesses meet the expenses and potential fines resulting from a suspected or actual breach of credit card data.

Merchants are eligible for three (3) levels of protection. By paying a low monthly premium PAI Secure will offer protection to help offset costs and expenses in the event of a data breach. Please call today to speak to a specialist who can assist you with determining your coverage.

The PAI PCI Secure Indemnification Coverage has optional coverage at up to \$75,000 or \$100,000 annually, with no deductibles and can be applied to the following data breach expenses:

- A Mandatory Forensic Audit;
- Required Card Replacement Costs & Expenses;
- PCI DSS Fines and Assessments;
- Fraud Losses Incurred at Other Locations Utilizing Cards Linked to a Data Breach at Your Business.

Step 4 – Network IP Scanning (may not be applicable to all merchants)

If SAQ C or SAQ D was completed, then a network IP scan is required and must be completed by a PCI Approved Scanning Vendor (ASV). PAI Secure has partnered with Security Metrics, a certified security assessor for Visa, MasterCard, American Express and Discover Card to complete your network scan. Once the initial scan is complete with a passing status, scans must then be conducted on a quarterly basis as mandated by the PCI DSS requirements.

Log on to www.securitymetrics.com and click the 'enroll now' button to get started.



**PAI Secure – covering all aspects of PCI requirements and more.
Another way PAI works for you.**

For questions about getting started please contact our PAI Secure Compliance Experts at:

866-275-5922

or

PAISecure@GoPAI.com

Additional resources and PCI Compliance materials can be found at:

- Federal Trade Commission www.ftc.gov
- Merchant Risk Council www.merchantriskcouncil.com
- MasterCard Worldwide www.mastercard.us
- PAI Customer Information www.PAICustomerInfo.com
- PCI Security Standards Council www.pcisecuritystandards.org
- Security Metrics www.securitymetrics.com
- Visa U.S.A www.usa.visa.com



Payment Alliance Intl - PAI Secure
1665 Palm Beach Lakes Blvd., Suite 200
West Palm Beach, FL 33401