

Card Processing and PCI Compliance Basics

In order to safe guard card transactions, new rules are being set by the payment card industry to tighten up and standardize how card processing is handled.

The Payment Card Industry (PCI) has implemented standards for secure card processing called Data Security Standards (DSS). The PCI group has created a special set of standards for software developers and integrators, like Atlantic Systems, that are known as Payment Application Data Security Standards (PA-DSS). The PCI-DSS and PA-DSS are collectively referred to as PCI Compliance standards.

Any business that processes credit and debit cards must become PCI compliant by July of 2010 or you may be subject to fines, increased rates and perhaps suspension of card processing altogether. Below are the 12 steps that must be followed to be compliant.

- 1 – Install and maintain a firewall.
- 2 – Do not utilize default security parameters provided by vendors.
- 3 – Protect any stored card data.
- 4 – Encrypt the transmission of card data during processing.
- 5 – Use and maintain anti virus software.
- 6 – Develop and maintain secure systems and applications.
- 7 – Make access to card data restricted to a need-to-know basis.
- 8 – Assign each system user unique ids and passwords.
- 9 – Restrict physical access to card data.
- 10 – All access to card data and networks must be logged and tracked.
- 11 – Test security and processes on a regular basis.
- 12 – Create and maintain policies that address information security.

Basically these rules cover 3 areas of your computer system:

- 1 – Network security (numbers 1,2,10,11).
- 2 – Internal store security and data access for employees (5,7,8,9,12)
- 3 – The processing of card transactions and storage of card information (3,4,6).

In order to become and maintain PCI compliancy you will be required to have PA-DSS compliant card processing software, fill out a PCI assessment document supplied by your bank or card processor that describes your security measures, and have your network security tested a minimum of 4 times per year by a certified testing company.

Atlantic Systems will be responsible for supplying you with a PA-DSS compliant card processing software interface. We can also help you check and/or obtain a PA-DSS compliant version of any third party card processing software. These would include RBSWorldpay (Lynk), Mercury Payment, and Verifone's PC Charge/IP Charge. You will be responsible for obtaining the services of a certified network testing company and arranging for regular testing. We can help with suggestions of where to find these.

For more information on PCI compliance go to www.pcisecuritystandards.org.

