



Standard Change-Makers, Inc.
3130 N. Mitthoeffer Road
Indianapolis, Indiana 46235
www.standardchange.com

What is PCI compliant or PABP compliant?

Do I need to be PCI/PABP compliant?

If you are a merchant or business owner that accepts credit cards, even if it is only a small part of your revenue, the answer is **YES!**

What is PCI compliance?

The buzzword going around right now is **PCI-DSS** (Payment Card Industry – Data Security Standard) or **PABP** (Payment Application Best Practices) compliant. It has every company that accepts credit cards concerned. Most don't understand what this compliance standard requires or why it's required. We will try to help you wade through the confusion...

We checked online at Wikipedia, and here is what they say about PCI-DSS:

*PCI-DSS stands for **Payment Card Industry Data Security Standard**, and is a worldwide security standard assembled by the **Payment Card Industry Security Standards Council (PCI SSC)**. The standard was created to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats. Any company processing, storing, or transmitting payment card data must be PCI-DSS compliant. Non-compliant companies who maintain a relationship with one or more of the card brands (Visa, MasterCard, American Express, Discover, JCB, etc.), either directly or through an acquirer risk losing their ability to process credit card payments and being audited and/or fined. All in-scope companies must validate their compliance annually. Auditors can conduct this validation - i.e. persons who are **PCI-DSS Qualified Security Assessors (QSAs)**, however smaller companies have the option to use a self-certification questionnaire. Whether this questionnaire needs to be validated by a QSA depends on the requirements of the card brands in that merchant's region.*

In essence, the credit card brands (Visa, MasterCard, etc.) have created this compliance standard to protect their cardholders' personal information from being stolen when their cards are being used at any place of business. With identity theft crimes increasing throughout the world, the credit card companies want to be sure that cardholders' personal information (such as name, address, credit card account numbers, security digits, etc) is not stolen during the processing of a credit card transaction. The card brands are putting the onus on merchants to protect this information.

The PCI-DSS/PABP compliance standard requires every merchant that accepts credit card payments to provide adequate security for their credit card customers. This would include having secured access to their computer network, firewalls that prevent outside intrusions, programs in place to be certain that cashiers properly dispose of any copies of complete credit card numbers (forms with just the last 4-digits are considered acceptable). The security standards are primarily directed at, but not limited to, merchants and internet-based merchants that process transactions using the internet - due to the risks of computer hacking into networks and servers. (There are some exemptions for dial-up processing at this time, but a QSA may be needed to determine if your dial-up terminal meets compliance standards, especially if any information is stored in a computer or hard copies are stored at your facility).

How do you get certified or approved for PCI/PABP?

The primary ways of providing banks with information that your company meets PCI-DSS compliance is to submit a completed **SELF ASSESSMENT QUESTIONNAIRE (SAQ)**, or to complete a Security Standards Audit by a certified **Qualified Security Assessor (QSA)**.

Here is a link for the SAQ: <https://www.pcisecuritystandards.org/faq/index.shtml>

Here is a link for QSA firms: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

Is my Standard Change-Makers machine PCI compliant?

In the definition of PCI compliant – the machine itself does not have to be compliant. It is the individual merchant that must meet the compliance standards. The machine card processing components must be approved by Visa as being compliance certified as a Validated Payment Application. Even if you own a machine that is certified for “PCI compliance”, that does not necessarily mean that you are compliant as a merchant (it certainly helps – but does not guarantee compliance).

In the case of the Standard Change-Makers’ credit card accepting machines, the change machine does not store or transmit any credit card transaction data. The information is passed through the card reader into the Datacap Systems’ **DataTran™ 162SL** POS (Point of Sale) Terminal device. The DataTran™ is the dial-up terminal and is programmed specific to the merchant’s information. The DataTran™ uses a phone line to communicate with the card processor’s server.

In cases of hi-speed internet processing, there is a Ethernet cable that links the DataTran™ to an **IPTran™** device. The IPTran™ digitizes the information for communication over an internet connection. The IPTran™ is typically connected to a PC that is connected to the internet; or connected to a network router that is connected to a cable or DSL modem (that is connected to the internet).

Both the DataTran™ and IPTran™ are on the Validated Payment Applications (VAP) List (see the web link below).

At this time in the process, QSA inspectors are primarily concerned with security of the internet or phone connection, and the storage of the information in a PC or server. Making sure that the information kept is secure from outside intruders or hackers.

NOTE: Merchants are required to prove they’re compliant with PCI/PABP on an annual basis.

How do I fill out my SAQ for my Standard Change-Makers’ product?

If you are doing a self-evaluation form, the Standard Change-Makers machine would be identified as the **POS** and the Datacap Systems DataTran 162SL would be the **FRONT END** of the POS.

According to the current guidelines, the DataTran™ must be PABP certified, and it is registered on the official list of Validated Payment Applications – shown on page 12 (as of Dec, 2008). Here is a link of the Validated Payment Applications list:

http://usa.visa.com/download/merchants/validated_payment_applications.pdf

Because the Standard changer does not store any card information - it is passed through the DataTran™ to the network processor’s computers – the card industry is not requiring Standard Change-Makers to certify our machine at this time. The approval of the DataTran™ is sufficient, because it is the component that stores and transmits the data.

You may provide this same information to your bank when they inquire about your change machine meeting the Validated Payment Application requirement for PCI compliance.

What happens if I don’t meet PCI compliance standards?

If you do not meet PCI compliance, you will be in conflict with your merchant agreement that states you will do everything within your power to properly protect your customers’ information from theft. In addition to you being terminated for credit cards acceptance, you can also be fined, hit with increased service and/or transaction

fees. It will be at the discretion of the organization that set up your merchant account whether or not any of these actions are initiated.

We are aware of a customer that was being charged \$120 per month by his bank, unless he could prove that his company was PCI compliant.

SCM REGIONAL SALES & SERVICE CENTERS

Standard Change-Makers, Inc.
3130 N. Mitthoeffer Rd.
Indianapolis, IN 46235
TF: 800.968.6955
PH: 317.899.6966
FX: 317.899.6977

Standard Change-Makers, Inc.
11731 Telegraph Road, Ste. A
Santa Fe Springs, CA 90670
TF: 866.394.5411
PH: 562.942.7188
FX: 562.801.1180

Standard Change-Makers, Inc.
2995 Dutton Mill Road
Aston, PA 19014
TF: 866.394.5412
PH: 610.859.0530
FX: 610.859.0627

www.standardchange.com