

How Do I Stay/Become PCI Compliant?

What is PCI?

The PCI DSS (Payment Card Industry Data Security Standard) is a set of comprehensive requirements for enhancing payment account data security. It was developed by the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis.

All merchants that process credit card transactions have contractually agreed to maintain and certify PCI DSS compliance as part of their Merchant Processing Agreement. If you only process ACH transactions, then the PCI DSS does not apply to your company.

What Do I Need to Do to Operate in a PCI Compliant Manner?

The PCI DSS consists of 12 key principles and accompanying requirements to which all merchants processing credit cards and service providers offering credit card processing services must adhere.

However, as a small business utilizing PaySimple for all payment processing functions, most of the very technical system requirements will not apply to you. The following are the key actions you need to take on a regular basis to keep your company compliant:

- Securely store all documents and files that contain credit card numbers.
- Never leave documents that contain credit card numbers in plain sight or unattended.
- Shred or incinerate any documents that contain credit card numbers when you no longer have a business reason to keep them.
- Never store track data from a credit card or the cvv2/cvc security code from a credit card.
- Limit employee access to credit card information on a need-to know basis.
- Use only unique username/password combinations to any software or system that stores or transmits credit card numbers, and NEVER share user accounts or passwords.
- For any computer from which credit card information is entered, stored, or transmitted, install a hardware or software firewall and implement virus protection software that is updated regularly.
- Adopt a security policy for your company that addresses storage, access, and transmission of credit card information. ([Get a sample here](#))
- Submit a SAQ (self-assessment questionnaire) certifying your PCI Compliance each year.

If your company directly stores or transmits credit card information from its own systems (entering transactions directly into PaySimple does not count), or if you process more than 20,000 Internet transactions a year, or more than 1 million total transaction a year, you will also need to have quarterly scans performed on all your IP addresses by a PCI Approved Scanning Vendor.

How Do I Certify PCI Compliance?

Each year you must complete a Self-Assessment Questionnaire (SAQ) and an Attestation of Compliance form and have it submitted to your credit card processor.

The way you process credit cards and store customer information will determine which SAQ you are required to complete. The simplest, the SAQ-A, is designed for MOTO merchants (mail order/telephone order/Internet) that do not transmit or store credit card numbers electronically from their own systems. ([You can see a sample SAQ-A here.](#)) Most PaySimple merchants that enter all transactions directly into our PCI-compliant system will fall into the SAQ-A category.

To find out whether you Qualify for SAQ-A, and to download the SAQ-A form, visit [PaySimple's PCI Compliance Center](#).

I Don't Qualify for SAQ-A, What Do I Do?

If you don't qualify for SAQ-A, you have two choices—certify PCI Compliance under a different SAQ, or change your business practices so that your company will qualify under SAQ-A.

The most common reason merchants don't qualify for SAQ-A is that they store credit card numbers electronically in Excel files, or in some other software application. Not only is this insecure, but it is unnecessary. PaySimple provides secure storage of credit card numbers in our PCI Certified system—take advantage of this valuable feature and with some minor operational changes, you can likely qualify for SAQ-A. Here's what you'll need to do:

- Import customer information, including credit card numbers, into PaySimple from your current file, then erase the file from your computer/server.
- Enter all new customers directly into PaySimple with their credit card numbers.
- Process all transactions directly from PaySimple—either one at a time, or via a transaction batch upload.
- Integrate PaySimple with other business software applications, if necessary, by exporting Customer IDs, and Transaction ID and status from PaySimple and importing and synchronizing with your other application.

Other reasons you may not qualify for SAQ-A include your use of the PaySimple API, your use of third party software packages, your yearly processing levels exceed those permitted for SAQ-A, or if you have a second merchant account that is not associated with PaySimple. If you do, then contact our Customer Care team and you'll be referred to a PCI Compliance program appropriate to your company.