PCI DSS Compliance

FAQ's

General Statement

One of Greater Giving's top priorities is investing in the highest level of PCI compliance to ensure the protection and safety of your donor's credit card information.

Greater Giving is a Level 1 vendor, the highest, most secure level of PCI compliance across all our platforms— so you know your data will be safe. Our technology and processes are reviewed regularly and undergo an annual audit by a PCI accredited 3rd party to ensure PCI compliance. We are also our own merchant provider, securely processing all your transactions.

Greater Giving will continue to deliver all products and services with the highest levels of value, security and compliance to our clients as it relates to PCI DSS and all industry standards.

FAQS

What exactly is PCI?

PCI really stands for PCI DSS, or the Payment Card Industry Data Security Standard. This standard is designed to create common industry security requirements. It consists of 12 basic requirements and is supported by over 200 detailed sub-requirements.

Who started PCI?

Originally, it was a collaboration between Visa and MasterCard; however, other card companies that operate in the US have endorsed the PCI DSS within their respective programs.

How does Greater Giving fit into PCI?

Greater Giving is certified compliant as a Level 1 Merchant, or Level 1 Service Provider. This means that we have submitted the following material as required by PCI DSS:

- An external audit, performed by a PCI Qualified Security Assessor.
- A quarterly network security scan report by a PCI approved vendor.

How can I see that Greater Giving has a current PCI rating/endorsement?

Visa maintains a registry of compliant service providers. You can confirm Greater Giving's presence by going to http://www.visa.com/splisting/index.html. Click on the yellow Search Service Providers button. Type Greater Giving into the Company Name field, and then click on Search, on the lower right hand side of the page.

How many levels does PCI recognize?

PCI recognizes four different merchant, or service provider levels, based on the number of card transactions processed annually. The transaction levels are based on both e-commerce (online) and other (card-present) transactions.

Is there other security/compliance documentation?

We receive three main documents as a part of the PCI DSS compliance process:
-AOC (Attestation of Compliance)
-ROC (Report on Compliance)
-Vulnerability Scan report

These documents are submitted to PCI as part of the annual compliance audit. For confirmation of our PCI compliance status, please refer to the Visa Global Registry of Service Providers at http://www.visa.com/splisting/index.html.

These specific documents however cannot be shared with a third party, because it would put our security infrastructure at risk. The SSAE 16 (Statement on Standards for Attestation Engagements Number 16) is available by request; which allows Greater Giving to show a third party we do have controls in place to protect data, prevent fraud, etc., without giving specific details which would compromise our security.

If I use Greater Giving, how is my donor's card data treated?

First, all card data is encrypted once the card is read by our terminal or card readers, using industry standard encryption technology. Second, while in storage in our databases, data remains encrypted with security standard certificates. This data is only stored for processing, and is then deleted, or reduced to just the first and last four digits. Security codes are never stored.

What about my donor's other info?

We only share cardholder information (card number, name, etc.), with the credit card processing networks. Only specific approved individuals within Greater Giving have access to that information, for legitimate business reasons – such as resolving cardholder disputes or refunds.

How does Greater Giving secure its servers and databases?

Physically, our servers are hosted in secured data center, which strictly limits access to the data center to authorized personnel.

Electronically, we secure access to our online applications using these industry standard practices:
1) Firewalls limit access from the Internet to our servers. 2) Our software is updated with the latest security patches 3) We monitor our systems 24/7 to ensure that our servers are operating at peak efficiency.

What if something happens and the servers go down?

Greater Giving has continuous backups of our server data for recovery purposes, which uses the industry standard encryption mentioned earlier. So, we're able to get back up and running as soon as possible.

How does Greater Giving keep the servers up and running?

We keep the servers up and running by using redundant hardware in the data centers. This means there are servers which automatically kick in to keep everything going if one server has issues.

The data centers also have backup power supplies and multiple internet connections from different providers, so a single outage can't interrupt your access to Greater Giving software and services.

Finally, backups occur every few minutes. We also have a daily backup, with the data being stored in a separate secure location.