Security, Privacy and Financial Transactions

Greater Giving Products and Services

September 2016

Security, Privacy and Financial Transactions

Contents

Greater Giving
1920 NW Amberglen Pkwy
Suite 140
Beaverton, OR 97006

www.greatergiving.com
Security, Privacy, and Financial Transactions, Page 2

Introduction

Greater Giving provides products and services to support nonprofit organizations and schools in their fundraising efforts. In the implementation of these offerings, Greater Giving manages organization and donor information and processes payments for clients. Ensuring privacy and security of the information is an integral part of Greater Giving's services and is the top priority for its operations. This document describes Greater Giving's security and privacy statements including the handling of financial transactions and how the data is protected from loss.

Security Statement

Greater Giving is in compliance with the Payment Card Industry (PCI) Data Security Standard.

The Payment Card Industry (PCI) Data Security Standard offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of collaboration between Visa and MasterCard and is designed to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs. The PCI Data Security Standard consists of twelve basic requirements supported by a total of more than 200 detailed sub-requirements.

See http://www.visa.com/splisting/index.html for reference.

Greater Giving has been certified as a Level 1 Merchant or Level 1 Service Provider with PCI. Hence, Greater Giving has provided the following material as required for certification with the PCI Data Security Standard:

> • External Audit by a Qualified Security Assessor According to the Payment Card Industry Data Security Standard
> • Quarterly Network Security Scan Report by Approved Vendor

The PCI Data Security Standard defines requirements regarding securing cardholder information, network security, encryption, data backups and disaster recovery, access control and monitoring, and vulnerability controls in addition to several other topics and is considered a state-of-the-art program for information security. Greater Giving fulfills the requirements as stated in the PCI assessment audit guidelines and passes the network security scans by PCI-approved security audit companies. Greater Giving used PSC as the PCI auditor, a leading security assessment company.

Greater Giving's security policy covers several hundred aspects of protecting data and avoiding fraud. Here are excerpts of the policy addressing frequently asked questions:

Greater Giving
1920 NW Amberglen Pkwy
Suite 140
Beaverton, OR 97006

www.greatergiving.com
Security, Privacy, and Financial Transactions, Page 3

Collection and Storage of Cardholder Information

Any input and transmission of Cardholder Information over the Internet is encrypted using strong, industry standard encryption technology. When Cardholder Information is stored in databases, the information is securely encrypted. All of the encryption methods use industry standard certificates. Cardholder Information is only stored for processing and then the data is deleted or reduced to the first and last four digits of the card number. Card Security Codes are never stored and are only used during the transaction and track 3 data from credit cards is not read.

Access and Sharing of Cardholder Information

Greater Giving's Online Applications will forward the Cardholder Information only to the credit card processing network. The only other access to the cardholder information is by select Greater Giving employees who require the information for legitimate business purposes, such as the resolution of cardholder disputes or to apply authorized recurring charges. This may involve sharing cardholder information with Greater Giving's credit card processor but there is no other sharing of the information.

Physical Access Control

The servers running Greater Giving's Online Applications and managing its data are in a hosted data center with physical access control in order to prevent theft of the equipment holding cardholder information. Only authorized personnel are allowed to enter the data center.

Electronic Security Control

The servers running Greater Giving's Online Applications and managing its underlying data are secured using industry standard practices. A firewall enforcing restrictions to the minimum number of ports open to the public Internet is maintained at all times by certified personnel. Server software is kept up-to-date with the latest security patches. Electronic monitoring tools send an alert on a 24x7 basis in case of non-responsiveness, high load conditions or other indications of penetration attacks. Administrative access to the servers is restricted to very few select personnel who have been screened for security concerns.

Data Archiving

Greater Giving performs continuous backups of the production data for recovery purposes. Any data backups of cardholder information are stored in a secure facility and are completely erased when they expire. The data on the archives maintain the encryption as defined above and are not allowing decryption from the backup media because it requires a separate security certificate.

Greater Giving
1920 NW Amberglen Pkwy
Suite 140
Beaverton, OR 97006

www.greatergiving.com
Security, Privacy, and Financial Transactions, Page 4

Protecting Sensitive Information

Only select personnel have access to sensitive information (including but not limited to card numbers, bank account numbers, agreements, client financial details, or other confidential information) and only if and when required for their job. If personnel receive sensitive information not required to perform their job, personnel shall inform the sender and intended recipient, if known, and permanently delete the information. Sensitive information shall be in direct possession or under lock and key at all times. In particular, sensitive information shall not be sitting on desktops while away from the desk. Sensitive information shall only be forwarded to other personnel if required by the job. Any copies of sensitive information that are no longer needed are shredded if in paper form or permanently deleted otherwise. Original records of sensitive information are only updated by authorized personnel.

Security Reviews

Greater Giving periodically reviews the use, procedures, and actual source code of Greater Giving products to ensure that there is no Trojan horse or other malicious use embedded in the product. The review is performed by independent personnel who are not involved in the development of these Greater Giving products. These reviews are scheduled quarterly.

Fraud Monitoring

Greater Giving uses certain heuristics developed specifically for Greater Giving Online Payments to detect fraudulent use. If suspicious transactions are detected, the client will be notified and further investigation will determine next steps.

Data Protection

Several of Greater Giving's products provide websites with attached databases to manage data for our clients. Protecting this data from loss because of server failures is part of the backup procedures and the business continuity policy.

Greater Giving runs redundant hardware in its data centers. This starts at the server level, where servers are equipped with hot-swappable redundant arrays of disk drives (RAID), multiple power supplies and multiple CPUs. Each critical server is accompanied with a stand-by server of the same configuration that can replace the server in case of a critical failure that the server level redundancy cannot recover from. The data center has backup power from generators and multiple Internet connections from different providers so that it is isolated from power failures and Internet connectivity interruption by a single vendor.

Greater Giving maintains two data centers and subscribes to a commercial backup storage service in order to protect the data. Incremental backups are run every 10 minutes and shipped to a secondary location. Furthermore, on a rotating basis, backup tapes are pulled once a day and stored in the secure commercial backup storage facility.

Greater Giving
1920 NW Amberglen Pkwy
Suite 140
Beaverton, OR 97006

www.greatergiving.com
Security, Privacy, and Financial Transactions, Page 5

Financial Transaction Handling

Greater Giving processes credit card charges from supporters for its clients either using credit card terminals at events or using online websites. The following describes the handling of those charges and their deposit into client bank accounts.

Greater Giving creates a unique merchant account with its processing partner for each client to ensure that each client's payment transactions are handled correctly. A few days after the credit card charges are settled, the payment processor transfers the funds to a special client trust bank account maintained by Greater Giving. The Greater Giving client trust account is only used for the purpose of handling client funds, issuing payments to clients and paying processing fees to the processing network. Client funds in this account are never used to pay any operating expenses and these funds are never intermixed with Greater Giving's operating accounts. Within the client settlement period defined in the agreement for payment services, Greater Giving transfers the funds, less the specified fees, due to the client directly into the client's bank account or by check.

Accurate and timely processing of the transactions are of paramount importance to Greater Giving's operations. Greater Giving selects its banking partners and payment processors based on their financial stability and maturity of their processing operations. Greater Giving's payment processors for credit card terminal and online transactions process millions of transactions per year on a worldwide basis and do so with high reliability and security. Greater Giving's banking partners are nation-wide public financial institutions with tens of billions of assets and operations well equipped to handle the financial transactions behind the payments related products and services that Greater Giving offers its clients.

Greater Giving has implemented an automated system that determines the transaction activity for a client, subtracts its specified fees, issues the fund transfer for the client, and generates a summary statement. Separately, clients receive transaction reports from their settlements either from the credit card terminal or through the reporting available in Greater Giving Online Payments. This allows clients to verify their summary statements of funds received.

Greater Giving has processed in excess of $4.5 Billion for more than 15,000 client organizations. Its system has handled more than 10,000,000 individual credit card transactions with no outstanding reconciliations.

Greater Giving
1920 NW Amberglen Pkwy
Suite 140
Beaverton, OR 97006

www.greatergiving.com
Security, Privacy, and Financial Transactions, Page 6

Privacy Statement

The following defines Greater Giving's policies for websites that it maintains either for its own purposes or on behalf of its clients.

> It is our policy that **no information of any kind** or from any source about visitors to this site, our clients or our clients' customers, **is sold or released to anyone** without the prior consent of the visitor, client or client's customer, or without a court order. This includes email registration to mailing lists, contact forms, and browsing logs. Reports of website visitor behavior are generated by our system. These reports contain personally identifiable information **only if you choose to identify yourself** to us.

Non-personally-identifiable Information Collected by Our Site

We collect the following types of non-personally-identifiable information about users who visit our website: your IP address (a unique number assigned to every computer on the Internet); domain type (i.e., .com, .net, or .edu.); and standard information included with every communication sent on the Internet. Information which we can infer from this standard information includes: your browser version and type (e.g., Netscape or Internet Explorer); operating system (e.g., Windows or DOS); browser language (e.g., Java); service provider (e.g., MindSpring or AOL) and; how you navigate the pages you visit within our site (e.g. which pages you view).

If your browser allows, persistent cookies are placed on your system. These cookies remain on your system and are automatically retrieved when you return to our site at a later time. It cannot be associated with an individual, unless you choose to identify yourself. Our site is designed to function equally well with cookies turned off. However, you may be required to sign in upon each visit if you have chosen this browser option. *Please note: We **never** place private data inside of these cookies. It is simply a convenient place to store a single identifier to help us recognize you when you return.*

A specific policy applies when Greater Giving maintains Web pages and processes data on behalf of its clients, in particular, when processing payments through credit cards:

> Your personal information will not be shared with anyone other than the client organization and the payment processor to securely process this transaction.

The following explains further details on use of supporter information provided to the client organization:

> Although Greater Giving consults its client organizations to adhere to standard practices in usage of the data provided, Greater Giving is not responsible for the information practices of its clients. Client organizations may collect information from or about supporters, including personal information. The collection, use, and disclosure of information by a client organization are subject to their respective privacy policies, which may differ from Greater Giving's privacy policy. Greater Giving encourages supporters to review the client organization's privacy policy before providing data.

Greater Giving
1920 NW Amberglen Pkwy
Suite 140
Beaverton, OR 97006

www.greatergiving.com
Security, Privacy, and Financial Transactions, Page 7

Finally, this policy protects the data owned by each client:

All data collected on behalf of one client is the property of that client organization and will not be shared with third parties except if required for use explicitly authorized by the client organization or if demanded by a court order. In particular, credit card information will be forwarded to the payment processor to securely process transactions.

This also means that all supporter contact information of one client is restricted in use to that client even if the same supporter is also participating in another client organization. Separate records will be maintained for each client's supporters and their activities.

Greater Giving reserves the right to use some of the data in aggregate for research, quality assurance, and statistical purposes. All information individually identifying either client organizations or supporters will be removed for the analysis and the results will be reviewed to preserve anonymity before publishing. If a client organization or a supporter provides permission to publish results of their specific activities, then Greater Giving might use those at its discretion.

Greater Giving
1920 NW Amberglen Pkwy
Suite 140
Beaverton, OR 97006

www.greatergiving.com
Security, Privacy, and Financial Transactions, Page 8