Privacy & Data Security Standards

October 2011

Your data is safe and 100% in your control in the Community Database Program.

- Your data is housed in a secure server; there are no unauthorized users.
- *Every trade is permission based* – each trade request is on a per list basis, meaning you control who uses which lists, and when.
- All trades are for one-time use only.
- Trade data may not be downloaded by the requesting organization. All trades will be routed through a mail house or through the managing partner organization (in the event that the organization does not use a mail house).
- Under no circumstances will the managing partner organization or TRG Arts share, deliver, or export any data or list from the compiled database without the express consent and permission of the list owner.
- While email addresses and phone numbers are accepted for use by the organization supplying the information, email and phone trades are not permitted within the system.

Safeguards Available

Change your Password

You are given a temporary password for your eMerge account. Each user within an organization is given the same initial password. It is very important to change this password the first time you log-in.

Assign List Exchange Approvers

- Designate which users at your organization are qualified to respond to trade requests.
    - TRG recommends you designate at least two list exchange approvers.
- Non-list exchange approvers may do everything in the system *except* approve or reject trade requests.

Deactivate Accounts

When an employee leaves your organization, please inform your TRG representative right away. The former employee's account will be deactivated and any new employee accounts can be created.

Hide Sensitive Lists

While trading within the system is entirely permission-based, you may decide to hide certain segments that you know you will never share. When a segment is hidden, your trading partners will have no idea it exists, and therefore cannot request it in a trade. Your organization is still able to utilize hidden segments for research, reporting and mail, email or phone lists.

Submit Suppression Lists during Updates

Suppression lists allow you to control who you and your trading partners can communicate with and through which channels. There are five types of suppression lists that can be used to remove patrons from any other lists in which they exist.

Privacy & Data Security Standards

October 2011

Patrons appearing in lists with the following buyer types are:

- SUP (Suppression) – Removed from all orders. This is the most comprehensive suppression buyer type
- DNM (Do Not Mail) – Removed from trades and mailing lists
- DNT (Do Not Trade) – Removed from trades
- DNE (Do Not Email) – Removed from email lists when 'List Use' is email
- DNC (Do Not Call) – Removed from phone lists when added to the shopping cart

Update Your Suppression Lists as Needed

When someone asks to be put on a do not contact list/do not trade list, you may add them to the appropriate list in eMerge. The Search/Add Suppress page, under My Account, searches the entire community database by last name and/or street name. This allows you to put names from house lists or names you received from trades on a suppression list. Make the change in your internal database as well.

Add Seed Names

Seed names can be thought of as decoy or dummy names. Creating seed names in eMerge allows you to:

- Add your name to any mailing list that includes your patrons' names
- Self-proctor within the system
    - Check on your mail house – Are pieces hitting houses when they should be?
    - Monitor how your names are being used in trade lists – Are they really mailing that black and white postcard?

Additional Information

Aggregate Data

TRG may utilize the Aggregate Data (data that has been processed by TRG so that it does not identify any individual person or organization) for research, but may not use, sell or disclose individual data without prior consent. TRG shall have the right to retain and use Aggregate Data for any purpose.

Web Security

TRG's eMerge application uses SSL (Secure Socket Layer) for requests via all web browser sessions. SSL is a process that encrypts data before it is sent across the internet, and uses a digital certificate provided by a trusted certificate authority. This process ensures the recipient can trust that the data was sent from a secure source when connected to TRG. TRG's Trusted Certificate Authorities are Equifax and Geo Trust, Inc.

Our eMerge Pro client interface sends data from the client site to TRG via SFTP (Secure File Transfer Protocol) requiring port 22 to be open for outbound traffic only. SFTP is based on SSH (Secure Shell) which is a network protocol that allows data to be exchanged using a secure channel between two networked devices. We also employ a robust firewall to protect data and software assets.

Privacy & Data Security Standards

October 2011

Since TRG does not accept, transmit or store any cardholder data, or financial information we are not obliged to operate under PCI Compliance guidelines—but we do take data security seriously. In addition to not storing any credit card information we do not store social security numbers.

Access to our servers and databases is limited strictly on a "need to know basis". Outside of access via our eMerge application, TRGs servers are virtually inaccessible outside of our internal corporate network and is protected with strict user authentication methods.

Each TRG server currently runs ESET NOD32 antivirus software to protect against virus infections.