VISIONS
Marketing for Credit Unions

Visions, Ink.
Mailing Database Security Information

Transfer of Data

Databases can be transferred to our Mailing department in the following ways:

- Electronically via email.
- Electronically uploaded to our FTP site.
- Via physical medium (CD, DVD, or thumb drive).

Customers are responsible for securing data during the transfer process. Suggested security methods are:

- Password protected file.
  - Bare minimum security if security is required.
- Zipped and password protected file.
  - Roughly equivalent to password protected file.
  - Zipping (compression) required for emailing larger databases.
- Zipped and encrypted file.
  - Higher security than password protected files and zipped/password protected files.
  - Standard security.
- PGP encrypted file.
  - Requires an exchange of security keys between companies.
  - High security allowing only those who possess the security keys access to the data.

Data Storage and Disposal

- All sensitive data files are processed for mailing on a single system.
- Sensitive data is stored on a 256-bit encrypted volume using AES-256 encryption with an SHA-512 hash.
- Unless otherwise requested, database files are retained for no longer than 2 weeks after mailing.
  - Requests for longer term retention will need to be made within 2 weeks of mailing or the files will need to be re-submitted.

105 Adelina Road, Suite 102, Prince Frederick, MD 20678
tel: 301.868.9577 | **fax**: 301.868.4937 | www.visionsink.com | info@visionsink.com