Frequently Asked Security Questions

- What is the general security environment for the eCHECKUP TO GO web site?
  - All eCHECKUP TO GO transactions are conducted across an encrypted 256 bit Secure Sockets Layer (Transport Layer Security (TLS)).
  - All drinking/drug use behavior data are stored on a secure server managed by the San Diego State University Research Foundation and are confidential and anonymous.
  - eCHECKUP TO GO user ID numbers are randomly generated 9 to 12-digit numbers.
  - The dedicated server is managed by the Interwork Institute at San Diego State University and updated regularly based upon the security guidelines of San Diego State University.
  - Access and error logs are analyzed and rootkit checks are reviewed by the system administrator.

- What are the security procedures and policies in place for the secure site hosting the application?
  - Server management is compliance with SDSU Security Policy (http://security.sdsu.edu/policy/secplan/drafts/index.html)
  - OS and installed software is regularly upgraded and patched.

- How and to what extent are the eCHECKUP TO GO hosts hardened against attack?
  - Firewalls are in place.
  - Reviews of logs and error messages.
  - Security patches applied as they become available.
  - Data coded to randomly generated user ID numbers.

- What database management system is the application data stored in? (Oracle, MySQL, etc.,)
  - MySQL

- Have the eCHECKUP TO GO Programs conducted a web code review, including CGI, Java, etc., for the explicit purposes of finding and remediating security vulnerabilities?
  - Yes; reviewed by the programmer and the sysadmin.
  - How often is this done?
    - Anytime there is an update, an error is detected, or upon customer inquiry.

- How do the eCHECKUP TO GO Programs handle backups?
  - Both the content of the site and the databases are backed up.
  - How often are they performed?

- Backups are performed daily by automated task and as needed by the programmer when the site is updated.
- To what medium?
  - SAN (Storage Area Network)
- Where are the backup media stored and secured?
  - In a secure, climate controlled, SSAE- 16-SOC 2 Type2 Compliant and Certified facility.

- What are the provisions for a subscriber to recover physical control of the data in the event the relationship with the vendor is severed?
  - Data will be delivered and/or deleted upon receipt of a subscriber's written request. The request must come from an individual authorized to make changes to the subscriber's account (i.e., a registered user).

- Can the eCHECKUP TO GO Programs immediately disable all or part of the functionality of the application should a security issue be identified?
  - Yes.

- How are credit card transactions conducted?
  - Our Credit Card processor is Elavon Virtual Merchant. If a subscriber does not wish to use our credit card processor, they may send a check to the address provided in the subscription agreement.

- What are the physical security precautions taken by the site hosting the eCHECKUP TO GO application?
  - Is there any power backup/redundancy?
    - Yes.
  - Is there any network redundancy/backup?
    - Yes.
  - Is there air conditioning redundancy/backup?
    - Yes.
  - How is physical access to the site controlled?
    - Access is limited to authorized individuals only. All entrances are monitored and security-card controlled.
  - How is network access to the application controlled?
    Is there a firewall, IDS/IPS, web inspection, etc.?
    - Software firewall, IPTables, is in place
    - SSH access is limited via DenyHosts to prevent brute force login attempts
    - SSH login/password is reviewed twice per year for password strength
    - Regular FTP is disabled for insecure file transfer