IOLTA Secure File Transfer Services

SAAS APPLICATIONS

Alvaro Flores | Steve Casey
ALTO SOFTWARE ENTERPRISE LLC | DELTA CONSULTING BOSTON, LLC

Table of Contents

OVERVIEW

Secure File Transfer is rapidly becoming the de-facto method for IOLTA programs to transfer and communicate information with third parties in a highly secure and efficient way.

With the increasing incidents of high profile data breaches, and the highly sensitive information that IOLTA programs receive from banks and other third parties, maintaining a highly robust and secure communications infrastructure is no longer viewed as optional by most IOLTA leaders, but rather, is critical to operating in the online world.

Fortunately, there are also now several powerful yet economical options available for secure file transfers that integrate easily and seamlessly into IOLTA program operations. The current options that we are recommending to IOLTA programs include the following:

1. IOLTA Secure Upload Site—with Optional Database Interface: This is a stand-alone website setup for the sole purpose of accepting file transfers, and sending them to a local destination at IOLTA, including the option to integrate transfers directly into an Information Logistics database (other database interfaces would be dependent on the ability of that software to integrate with the external site).

2. IOLTA Secure Communications Platform: This option allows for secure email as well as secure document transfer, which can include remittance data, as well as other information that needs to be sent securely to or from an IOLTA program. The secure communications platform employs an online file server dedicated to providing these communication services. This is a robust and flexible solution now in place at several leading IOLTA programs.

3. IOLTA Secure File Transfer Service: This option is a dedicated online file storage system with secure upload and desktop file replication, ideally suited for bank remittance reporting. Bank (or other secure) files are never handled by the IOLTA program until they show up in the banks individual folder on the user's desktop drive. This solution is the most cost effective, provides extreme operational efficiency, and has recently been implemented with great success for IOLTA use.

Following is more detailed information regarding each of these options.

OPTION 1. IOLTA Secure Upload Site

IOLTA remittance data and other information received from third parties is often sensitive and confidential in nature. The IOLTA Secure Upload Website is hosted on a server that is separate and distinct from the server running the IOLTA Management System (for security reasons).The following sections describe the typical functioning of the secure upload site, but each installation is fully customizable based on the IOLTA client and their particular needs.

For an example of the look and feel of this site, please visit the Louisiana Bar Foundation secure site at: https://lbfsecure.ilchost.com/

Product Highlights

Register

Banks / qualified institutions can use this form to request a login for the IOLTA Secure Upload website. This form requests the following pieces of information (all fields are required):

- Name
- Company or Organization
- Email Address: Validated to ensure that the entry is of a valid format.
- Phone
- Comments

Upon submission of this form, the contents are emailed to a designated IOLTA email address. The user is presented with a confirmation that their submission was successful and that IOLTA program will be in touch with their requested login information.

Login

A user must submit a valid username and password to gain access to the system. If an invalid username and/or password is entered, the system displays an error message and disallows entry into the system. Once the user enters a valid username and password, they are presented with the Remittance File Upload screen.

Remittance File Upload Screen

User is presented with a file-upload utility, allowing them to browse to a file on their local PC and select it for upload. Upon pressing the submit button, the system conducts the following checks:

- File Size: Maximum 10 MB allowed.
- File-Type: zip, txt, csv, xls, xlsx, pdf, doc, docx file-types allowed.

If the above checks pass, the file is saved to the server and the user is provided a confirmation message that their file upload was successful. Otherwise, the user is presented with an appropriate error message and the File Upload dialog is displayed for retry.

Associated Screens / Functionality in the Internal IOLTA Software

To provide a seamless experience for the IOLTA staff, new functionality will be added to the internal IOLTA software for managing banks' access to the Remittance File Upload website as well as display and download of files uploaded by the banks.

A new "Manage Remittance File Upload Website Login" section can be added to the internal IOLTA software system. Here, an IOLTA staff person can specify a username and password (or modify the existing username and password) for a given bank.One set of credentials is setup for each bank, meeting secure complexity requirements.

IOLTA staff will distribute login information to the Bank Contact, offline.
To remove access for a given bank, the staff person simply clears the username and password fields here and presses the Save button.

A new "Remittance File Uploads" section can also be added to the internal IOLTA system software. Here, an IOLTA staff person is provided with a listing of all the files that were uploaded by a bank in chronological order. Staff will have the option of downloading these files by clicking on the links provided. Delete links are also displayed for each file listed to allow a staff person to delete a file from the Remittance File Upload website.

Secure by Default

There are several levels of data protection provided by the secure upload site:

- Access to the Remittance File Upload Website is done through an SSL session (https://) which automatically encrypts all transmissions between the user's web-browser and the server using a 2048-bit key. Incoming Port 80 traffic (http://) will be re-routed to avoid any unencrypted transmissions.

- The virtual hard-drive that houses the web-server and database will be fully encrypted employing the strongest encryption algorithms that are available to provide a very high level of security for the data stored on it. If an unauthorized user gains access to the virtual hard-drive, the contents of it will be fully encrypted and the data rendered useless.

- Database level encryption is also done to mask account-numbers as they are stored within the database. The accounts will be decrypted after they are retrieved from the database to display on the IOLTA users' web-interface. Any new accounts that IOLTA users add into the system will be encrypted before they are stored within the database.

- A Hardware VPN is an additional option for an even higher level of security between IOLTA and the online servers.

Summary

For IOLTA Programs looking for a fully functional external website to manage their incoming secure file transfers, and with an unparalleled ability to integrate securely into the internal IOLTA management software, the IOLTA Secure Upload Site is a powerful option.

OPTION 2. IOLTA Secure Communications Platform

This Secure File Transfer Agent is configured to initiate the communication between clients at either end via https encryption.

For an example of the look and feel of this site, please visit the Texas Access to Justice Foundation secure site at: https://sfs.teajf.org/. A sample of the unique Filedrop page can also be found here: https://secure.filetransferagent.com/filedrop/example

Product Highlights

- Send Unlimited Sized Files to anyone using a simple Webmail-like Interface
- Receive Unlimited Sized Files from anywhere using modern and legacy methods.
- File and Folder Sharing with internal and external teams.
- Request Files with a simple link for the receiver to use when responding to the request.
- Emaildrops - Receive Files Securely using email with additional tracking.

Secure by Default

Encrypted — All files are transferred with Strong 256 bit FIPS approved encryption.

Authenticated — All downloads are authenticated ensuring that only the intended recipient will receive the files. Even Unauthenticated messages are protected using Strong Random Numbers to ensure only recipients with access to the secure link will be able to access the message.

Audited / Logged — All transfers are logged, giving you proof of any files sent in and out of the organization.

Compliance (HIPAA, PCI)

By using Secure File Transfer Agent, users will be able to send large files securely within the organization, to customers, contractors, accountants, banks, and all other parties requiring secure communication.

It will also help achieve Policy Compliance for Sarbanes-Oxley, HIPAA, PCI and other standards by encrypting sensitive data in transit, provide cryptographically strong random access keys for accessing transmitted data, and achieve non-repudiation with download receipts of who download what, from where (even by mapped locations) and at what time.

Outlook Plugin

Using the Outlook plugin, it's never been easier to send files. Click Secure Attach instead of attach in Outlook and you are done! By default, files will also automatically use Secure File Server if any file attached is larger than 20MB - you can set this limit to anything you want.

Intended Use

The Customer may only use the Enabling Code and Licensed Service to enable visitors of the website/application to send and receive e-mail messages and electronic files to the Customer's SaaS application in accordance with the Service Specification on the agreed website's domain once the visitor has activated the account by confirming the automated e-mail message and displayed by the Enabling Code.

For avoidance of doubt, all other uses of the Licensed Service are not seen as Intended Use.

Requirements

User should have installed the following to fully utilize all of Secure File Transfer Agent features

- Windows XP or later
- .NET v4 or higher
- Microsoft Outlook 2003 or later
- Internet Explorer 8, 9, 10 and 11
- Google Chrome
- Firefox
- Safari 6 and 7

Product Hosting

Secure File Transfer Agent is *SaaS* (software as a service) application and it is compatible with any browser. The Product is hosted in a high-security environment with a high level of redundancy and failover capabilities.

- Double redundant enterprise failover
- 100% Gigabit network (internally and to the Internet)
- Redundant power supply
- Highly scalable and high availability design
- Environmentally friendly
- Storage Area Network (SAN) storage over multipathed Gigabit iSCSI
- UPS and Diesel generator power backup
- 24/7 video and audio surveillance
- Level 3 security
- Aragonite-based automatic fire-fighting system
- Automatic server monitoring every 3rd second with alarm system
- Automatic daily backup

Product Features

Sending and Downloading Files with Ease
Uses a simple, easy to understand, webmail-like interface for sending files.

- Unlimited Files Size.
- Modern HTML 5 upload mechanism where supported.
- Automatic Fallback to HTML 4 where needed.
- Support for the 4 major browser vendors with their last 2 major releases (last 3 for Internet Explorer).

- Splits files in 100Mb blocks during uploads to get around proxy limitations.
- No Flash, Java or any other plugin used to send or download files.
- No browser tweaks or browser reconfiguration required to send or download files.
- Each message is sent with an expiration date, the message cannot be viewed and the files attached will be automatically deleted on expiration.
- Messages can expire on a certain date or after a set number of downloads.
- Multiple files can be automatically zip'ed and downloaded as one zip archive.
- Can set forwarding permission to control who other than the specified recipients should be able to download the files.
- Can limit message size on a per group or per user basis.
- Can BCC myself (to add to my email clients Sent folder).
- Can send files that have already been sent again without re-uploading.
- Can block files based on file extension or only allow files to be sent with certain extensions.

Receiving Files as easy as possible

- Users can receive files from external parties with no prior registration.
- Users can Request files from external parties that won't need to register to send files back from the request.

- **Filedrop pages** static URLs for receiving files A Filedrop page is a unique URL like https://secure.filetransferagent.com/filedrop/example, where the recipient is pre-set and the sender can be anyone.
- Requires no registration for the external party to use.
- User can have as many Filedrop pages as needed.
- Each Filedrop page has their own settings for restricted file types and max file size.
- Each Filedrop page can have individual forwarding permission to restrict who can download the sent files.
- User Filedrop pages — each local users can obtain their own static URL they can share in their email signature and is unique to them.
- User Filedrops can use a nice looking URL with the users email in the URL, a secure random string or both, as required.

File Requests one time file receive

- A File Request is a one-time file request users can send to any user. The recipient of the file request will get a one-time use link they can use to send files back to the requester.
- Requires no registration for the external party to use.
- One time use so it can never be abused.
- File Requests can be enabled on a per group basis.

Automatic Virus Scanning — All files are Virus Scanned when uploaded and deleted if found to be infected. You can integrate with your own custom file scanning and you can limit what types are files each user is allowed to send.

Security protects the user even when they do not realize it

- Secure by Default deployment.
- Can be deployed with no cloud interaction for maximum security.
- Built-in Firewall configured and enabled for maximum security.
- Can be deployed on the Internet with no other firewall or other protection.
- Minimal installed packages in the operating system configuration.
- All transfers can be required to use Industry Standard HTTPs.
- Only Strong SSL algorithms enabled.
- Only Strong SSL versions enabled.
- Protection from Cross Site Scripting (XSS) attacks.
- Protection from Cross Site Request Forgery (CSRF).
- HTTP Strict Transport Security (HSTS) enabled.
- All Downloads protected with 3 x 128 bit random tokens (384 bits).
- FIPS140-2 enabled OpenSSL for cryptographic functions (as opposed to weak standard system functions).
- Option to deploy using built-in full disk encryption for data-at-rest encryption.
- All files are protected for integrity using SHA-1 hashes.
- SHA-1 hashes are visible on all emails sent, on the message page and download information page.
- Can be configured as a closed system with no external user access.
- Passwords are never sent in cleartext.
- Custom Password complexity validation.
- User accounts can be configured to automatically be deleted after a number of days without activity.
- Default to not require external users to have accounts, and still provide authentication.
- Can require all users to have accounts.
- Strong 2-factor authentication can be enabled.
- 2-factor authentication can be enabled on a per group or per user basis.
- Secure local password store using the Bcrypt method.
- Single Sign-On (SSO) Integration with SAML 2 providers.
- Simple SSO integration with static shared secrets for simple local integration.
- Spam Protection without CAPTCHA — use of hidden fields in forms that bots will fill in but hidden from users with stylesheets.
- Brute Force Protection — default to block the ip address from the attacker for 15 minutes after 5 failed attempts within 5 minutes.
- Possible to block groups of users to only login from certain ip address ranges.
- Possible to block administrators to only administer the system from certain ip address ranges.
- All activity is logged. This include sending files, downloading files, successful and failed logins, creation, deletion and updates of user accounts, changes to any configuration.
- Can export all logs using Syslog.
- All files are scanned with ClamAV Antivirus on default.
- AV signatures is configured to update every 2 hours.
- AV Engine is configured to update nightly.

- Ability to add custom file scan (for integration into other AV engines, DLP solution and similar).
- Ability to limit forwarding permissions on a per group basis.
- Ability to limit recipient email domain on a per group basis.
- Ability to limit file extensions or only accept certain file extensions on a per group basis.
- Remember-me can be configured to not enabled, 2 weeks or indefinite.
- Geoloction and Google MAPS integration to get a visual representation of where a file has been downloaded from.
- Display Browser and Operating System details for downloaded files.

Branding and Localization

- Can be configured to look completely like an internal company system.
- Can be configured with no vendor branding visible to the end user at all.
- Ability to customize the front page with own logos and information.
- Ability to customize the header and title with different branding names.
- Ability to use own page footer on all user visible pages.
- Ability to insert custom Stylesheet to change the visual appearance of all visible user pages.
- Ability to insert custom JavaScript to change the behavior of all visible user pages.
- Can change any text or form label on any user visible page.
- Can change all emails sent from the system.
- Will detect system locale from the end users browser and display all pages in that locale (if available) with a fallback to English.
- Will detect the end users time zone and display all times in that time zone, with a fall back to a selectable user default time zone.

OPTION 3. IOLTA Secure File Transfer Service

Product Highlights

Overview

To facilitate the receipt of electronic remittance files from participating financial institutions in a secure, efficient and cost effective way, the Secure File Transfer Service is implemented in the following way:

- We will setup a customized on-line file transfer service using Files Anywhere enterprise services as the technology vendor. We have used Files Anywhere for our own business for nearly 10 years with excellent results. Files Anywhere has been in business since 1999 and boasts many customers in the fortune 100 and other large, highly secure businesses such as Deutsche Bank, CitiBank, and General Electric.

- Files Anywhere file transfer service is uniquely suited for the bank transfer application because it allows a fully customizable online environment, government level security protocols, and a seamless, single link upload option for each participating bank.

- For this custom application, Delta will setup an online environment that is specific for the particular IOLTA program and its needs. Each participating bank will have its own individual online folder to which it will upload its remittance file each month. We will create an individual link for each bank folder, as well as a secure password. As part of an IOLTA mailing, banks will be provided with these credentials as well as the simple instructions required to upload their monthly remittance files. We will also provide the IOLTA Program with a spreadsheet with the credential information (in the event that banks require it at a later time); links can also be recreated at any time, or new banks, folder and links added when necessary.

- Once the banks begin using the File Transfer Service, the IOLTA program will require very little interaction with the system. The online folders are replicated by a service running on the desktop called “CloudSync”. CloudSync uses technology similar to Google Docs or DropBox to create an exact duplicate of the online environment. As a result, each bank folder is replicated in the CloudSync Folder and the IOLTA user has immediate access to it for processing. There is no manual download required—no searching for files or emails; all bank uploads go into their own specific folder for THAT bank.

- The online bank directory can hold a significant amount of history without the purchase of additional storage (we are estimating that at least 5 years of remittance files for the average program can be maintained within the base configuration), with additional storage available at very reasonable costs. This should provide an attractive alternative to costly on-premises storage, and at a minimum a full backup of that data in an online data center environment.

- Even though it will not likely often be needed, IOLTA staff will have 24/7 access to the online banking directory via their own account and secure credentials. When a new remittance file is received, an email can be generated notifying IOLTA about the name of the file (using a convention similar to: "bank name/period") and the location where it was uploaded (e.g. \BankOne\). IOLTA staff can then retrieve the file in the CloudSync directory. There is also an online history of all files uploaded, including date and time, filename, and source of upload, that can be sorted chronologically or by file name, etc., so that a complete history of all files is maintained and easily retrieved.

- We will setup the messaging within the service is specific to IOLTA (the online branding is called "IOLTA File Transfer Service") so that bank's should be comfortable using it. Uploads of course are fully encrypted and specific messages can be added for contact information—all to insure the smoothest process possible for the banks and the fewest questions and complaints to IOLTA. Again, each bank will have its own unique link such that by clicking the link will bring them to a simple upload screen, where within a couple of clicks they can upload their file, which is then deposited into their specific bank folder for near immediate retrieval by IOLTA.

- On an ongoing basis and at no additional cost, we will insure the file system, links, messaging, security and backups are all working properly. In addition, we will setup any new banks up on the system, troubleshoot any upload/download issues and provide whatever other support IOLTA might need.

Basic Features (not all are applicable to this application)

- **No File Size Limit:** There is no limit to the size of the files uploaded/downloaded or sent from your account.

- **Receive Large Files from Non-Members:** Receive large files and entire folders though fully customizable FileReceive links to non-members. Secure your links by enabling password protection and auto-expiration. Keep an audit trail by tracking each activity and receiving automatic new file notification.

- **Password Protected Sharing:** Users can protect the links they send out with a password, thus, securing their shared downloads and ensuring safe delivery to the recipient.

- **Mobile Access & Apps:** Download mobile apps for your smart phones or tablets, or use your mobile browser. Never be without your files anywhere you go.

- **Point-in-Time Data Restore:** Snapshots of all accounts are taken at 11:00PM every day and are stored for thirty days. These snapshots can be used to restore data which may have been accidentally deleted.

  - **Virtual Folders:** Enables users to create a folder to store all of their frequently accessed items without rearranging the folder structure as a whole. This virtual folder is useful for creating a favorites folder or grouping sets of data.

  - **File Tracking:** Maintains a record of actions performed in the account e.g. files being moved, deleted, uploaded and edited. Never wonder what happened to a missing file or how a file was mysteriously downloaded.

  - **File Versioning:** Saves older versions of files when new ones are uploaded or the file is edited or altered. Stop worrying about overwriting files and losing important data on the old version.

  - **Disable Delete:** Option, to safeguard specific folders.

  - **Guest Subfolders**: Create subfolders automatically when guests upload files to your account.

- **View-Only Access**: Protect files while sharing by disabling downloads and printing. Place a "Confidential" or custom watermark on any document or image being shared.

- **Upload-Only Access**: Protect files in your account by providing upload only access.

- **Search Metadata & Tags:** Use the search function to search by Metadata or Tags applied to any files or folders. The search offers multiple ways to quickly and efficiently sort through your data.

- **File Preview:** View documents, videos, music or other files in your account, online, right in the browser (without downloading them).

- **Auto Expiring Links:** FileShare and FileReceive links can be set to expire automatically. The time of expiry may be set at the user's discretion.

- **Convert Documents & Images to PDF:** Convert documents and images to pdf format, without downloading them, right from your account.

- **File Lifecycle Management:** Users can define global purge rules that will delete files after a specified period of time. The lifecycle rule is useful for removing data that becomes sensitive after a certain period of time.

- **Manage Folder Access Keys:** Allows automated programs to upload files into a destination folder without requiring login credentials.

- **Upload Entire Folders:** Using the Multi-upload feature, users can transfer the entire contents of a folder (including subfolders) from their local computer to their FilesAnywhere account (while maintaining the original folder structure). Users can even drag and drop files on to the FilesAnywhere interface from their local computer and upload multiple files with just one click of the mouse.

- **Context Menu:** A right-click menu provides an easy to use interface for performing common tasks.

- **Service Plugins:** FilesAnywhere Service Plugins add even more great features to your account. You can enable or disable from any of the included services e.g. FilesAnywhere Fax Service, Zoho Editor for Spreadsheets, Documents, Slideshows, Aviary Photo Editor, Blogger.com

Posting, Autodesk Engineering Drawing Viewer, WordPress.com Posting and Twitter Backup.

- **Folder Contents Report:** Export the contents of your folder in excel format.

- **Folder Tree View:** Easy to use file and folder structure. Create and organize multiple layers of folders for all your content.
- **Graphical View**: View your files grouped by Tags, File Type, Extension, Size, Year, Month or Day.

- **Email Notifications:** Users can customize and receive email notifications on activity in their account.

Advanced Features

- **FTP, SFTP, SSH, SSL/TSL:** Connect to your account using different connection types. These methods offer reliability, security and the freedom to use your favorite SFTP client.

- **AES 256 Encrypted Backup:** Rest assured that your files are secure in the cloud encrypted with a strong 256-bit AES algorithm.

- **Automated Backup**: Using our CoolBackup program users may create multiple profiles to automatically backup local files to FilesAnywhere. Run backup jobs as a Windows Service.

- **CloudSync**: Easily synchronize files and folders from your FilesAnywhere account to your computer.

- **WebDAV Drive Mapping:** Access your cloud storage just like a local drive. Directly open and edit remote files using WebFolders.

- **At Rest Encryption:** Files are safe and secure at rest using an AES 256-bit encryption.

- **Role-Based Access Control**: Role-based security is implemented in the administration console for Professional and Enterprise accounts, in the form of Group-to-Folder permission assignments. Role-based-access-control (RBAC) is a widely accepted security control standard, reducing the time to apply and accurately maintain user permissions on specific folders, by assigning predefined lists of users with authorized access (also known as an ACL or Access Control List).

- **Audit Logging: Track every single activity on a file.**

- **Security & Permissions:** Assign which folders, individuals and user groups can access. Designate access permissions, including Master Access, Full Access, Create and Update, Read Only, Preview Only and Upload Only. Decide what permissions users can grant on shared files and folders. SSL encryption on data transfers is standard with every account. Get 256-bit AES encryption at rest for professional and enterprise accounts.

Secure by Default

Security Protocols

Is your data safe with the IOLTA Secure File Transfer Service? Absolutely. Since 1999 FilesAnywhere, has gone beyond standard measures to protect our customers and their data. Our unyielding commitment has made safe cloud storage possible. Thousands of businesses and individuals around the world use FilesAnywhere to store, access, and share data online. We deploy a blend of security measures to ensure maximum protection and the greatest overall data safety.

- **Independent Security Evaluation** - SOC 3, ISO-27002, and HIPAA Compliant.

- **Three-Tiered Testing** - Rigorous QA processes to eliminate errors.

- **Data Encryption for Transfers** - 128/256-bit SSL is standard on every account.

- **Data Encryption at Rest** - Isilon proprietary storage cluster data encryption comes standard on business and enterprise accounts.

- **Firewall Protection** - IP authentication and brute force attack prevention.

- **Automated Backup** - Coolbackup encrypts data locally before uploading with AES 256-bit encryption

- **Daily Snapshots and Data Restore** - Taken each morning at 5:00 a.m. and stored for 30 days of point-in-time backup.

- **Role-Based Access Control** - Advanced user provisioning and permissions.

- **Data Center Monitoring** - State-of-the-art facility with 24/7/365 monitoring.

App & Network Security

In today's online environment, customers demand security. We take your privacy, and the safety of your data, very seriously. Grant folder and file access to users, groups, or guests. Create virtual folders that allow for hand-picked file access. Add an extra layer of security with optional link-based password protection, link expirations, and lifecycle rules for automatic deletion of folders and file. In addition, McAfee Virus scanning of all files and documents comes standard. In short, we employ best practices for total assurance.

Account Security

- Administrative auditing and reporting
- Access and usage metrics
- Automated email notifications
- Custom password lifecycle
- Custom password strength requirements
- User level provisioning and permission levels
- Division, department, and group segmentation

Network Security

- Server protection by industry standard firewall
- Access restricted to fixed IPs
- Regular external intrusion testing
- Redundant backbone connections for high performance connectivity
- Intrusion detection system monitored 24/7/365

Data Center Security

We've applied an extensive and meticulous level of security to ensure the safety of our customer's files. Our data center is contained inside one of the best-connected hosting facilities in the world and is SOC 3 compliant. This state-of-the-art, telco-class facility offers complete redundancy in power, HVAC, fire suppression, network connectivity, and security. Every item of hardware and every connection is monitored 24/7/365.

Redundancy and Fault Tolerance

- N+3 redundancy to prevent single point failure.

- Rack mount hard drive arrays running RAID 50 provide continuous hot-swap disk redundancy.

- Multiple layers of power redundancy prevent downtime from power loss to servers, storage, and networking equipment.

Version Integrity

- Enterprise accounts are protected by 125 separately saved versions.

- Standard 30 days of automated backups for all accounts.

- Users may opt to configure additional Version History protection.

Intrusion Detection and Prevention

- Advanced multi-tiered security protocols are working together in layers to protect the network at all times.

- Firewalls monitor each firebox firewall appliance.

- Security monitoring software running on server equipment includes intrusion detection, virus scanning, system logs, and provides notifications of suspicious activity in real-time.

- Protection from email attack, spam, and viruses.

- Daily vulnerability assessments track deviations from standard baseline, presently protecting our network from over 40,000 known vulnerabilities.

Highly Trained, Expert Teams

- Our information security team includes engineers trained in data security, encryption, risk prevention and incident response.

- Experts in security methodology, threat avoidance, detection, and response.

- ## Compliance

Insufficient data management, ineffective workflow, transparency, and non-compliance are all problems that face companies today. Legacy systems require that the solution be molded to fit the problem. Private clouds are replacing traditional, on-premise systems from small businesses to large enterprises, and streamlining inefficiency. Even highly regulated industries, including financial services and healthcare, are able to migrate when data privacy, security implications, and legal and regulatory requirements are met.

Our approach to security standards is simple—to make sure our practices are even more thorough and more sophisticated than the customers we serve. Our data center is SOC 3 compliant meeting stringent criteria, and we have deployed security, encryption, and monitoring features within the application to help clients to meet the compliance requirements, including:

- HIPAA
- GLBA
- SOX
- SSA16
- PCI
- ISO27002

> *We employ the best practices to provide total assurance, delivering information privacy and standards compliance for our customers.*

Summary

Whether your IOLTA Program selects the Secure Upload Site, the Secure Communications Platform, or the Secure File Transfer Service, will depend on the specifics of your IOLTA program, your needs and priorities, and of course budget (although the latter two offerings are very economical even for small IOLTA programs).

We hope the above information helps in explaining the different offerings for securing your IOLTA information. In addition, we would be happy to schedule a demonstration of these services and further discuss their features and benefits directly with you at any time.

Finally, because we are aware how devastating a potential data breach would be, we urge you not to delay in implementing one of these secure options. Again, these days it is no longer a luxury to secure your sensitive IOLTA data, it is a responsibility and a requirement.

Our contact information appears below.

Thank you for your interest in the IOLTA Secure Transfer Service options.

Sincerely,

Alvaro Flores
ALTO Software Enterprise

al@altosoftwareenterprise.com

www.altosoftwareenterprise.com

Steve Casey
Delta Consulting Boston, LLC

Steve@deltaboston.com

www.deltaboston.com