


Rest Assured



There is nothing more important to ByAllAccounts than protecting the privacy of its customers and safeguarding their personal and financial information.

[More Security Information :: Click Here](#)



Security and Privacy Overview

Version 3.12



Overview	3
Security	4
Physical Security	5
Network Security	6
Software Security	7
Digital Certificates	7
Secure Connection - HTTPS	7
Session Management	7
Data Encryption	7
Application Features	8
Employee Policies	9
Privacy	10
ByAllAccounts' Privacy Statement	10
What type of personal information will be collected?	10
What information is collected for on-line account access?	10
Are Cookies Used?.....	11
How Does a User Discontinue Service?	11
Security Statement	11
128-bit Secure Sockets Layer (SSL).....	11
Physical Security	11

Overview

ByAllAccounts data gathering technology captures and manages highly sensitive information, including:

- names
- email addresses
- login IDs
- passwords

ByAllAccounts places great emphasis on safeguarding this information and maintaining a high level of security around it. ByAllAccounts employs industry-leading technologies and policies to protect the confidentiality and privacy of each user's financial and personal data. ByAllAccounts vigilantly updates its systems to stay at the forefront of security, privacy and continuity protection.

This document describes the security measures including physical protection of information, handling of disaster recovery and insured continuity of service, as well as ByAllAccounts privacy policies.

Security

ByAllAccounts has created a high-security environment designed to insure the privacy and security of its clients and their data. To assure this security, ByAllAccounts employs a number of different technologies including:

- Network security
- Application security
- Encryption

All personal user information is stored in an encrypted format in the ByAllAccounts database, and is transmitted in that encrypted format within the network.

Production systems are housed at a site that provides state-of-the-art security, redundant power, redundant high-speed Internet connections, system monitoring and management, comprehensive backup, and disaster recovery.

ByAllAccounts performs extensive security checks on its employees and has implemented stringent internal controls with regard to sensitive information.

ByAllAccounts has its security and privacy policy and procedures reviewed by independent auditors on a periodic basis. In addition, ByAllAccounts keeps access logs and other historical information to provide clear audit trails.

This document is intended for general distribution. It is important to note that as part of the overall security process, ByAllAccounts does not provide specific details regarding its security procedures and processes in this public document. ByAllAccounts would be happy to discuss any questions or concerns regarding its security, backup, or disaster recovery plans and processes or the security vendors we employ.

The following sections provide a further level of detail regarding the ByAllAccounts security processes.

Physical Security

The ByAllAccounts servers and database of user information are physically protected at a highly secure site. This site is protected from outside access by a series of firewalls and a comprehensive suite of security products. The physical premises are internally monitored twenty-four hours a day by security personnel. Only a very limited number of authorized personnel are granted access to the data center, and only after successfully passing multiple forms of personal identification and access authorization verification.



The following additional security measures are in place:

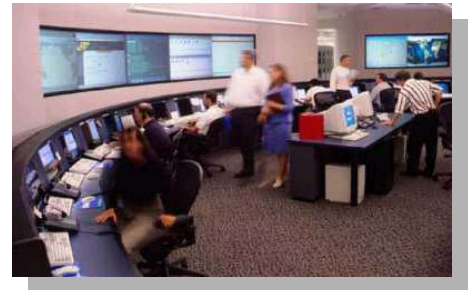
- Video surveillance monitored security personnel and recorded
- Access controls to machine rooms that are separate from access controls to the building.
- Access controls to server cabinets that are separate from access controls to the building and to the machine room.
- A limited number of designated ByAllAccounts employees have access to the production machines
- Permanent record of all access is logged electronically and on paper

Network Security

Systems on which ByAllAccounts' service runs are dedicated exclusively to the service. No additional software, including debugging software, is permitted on any production system.

The ByAllAccounts data gathering technology requires limited, well-defined access to and from the Internet. Inbound access is only permitted to the web servers, which are physically separate from the other components, and open ports are limited to HTTP (80) and HTTPS (443). All other ports have been closed down as part of the system design.

ByAllAccounts uses only state-of-the-art equipment from proven, mainstream vendors, such as Cisco, Sun, and EMC, to provide secure hardware environments. Additional network-level security includes anti-spoofing, secure DNS, and anti-virus via 24x7 monitoring. Log rotation is also in place to allow access to past events. Remote access is limited via VPN and two-tiered login.



Software Security

ByAllAccounts implements a number of security measures directly in its software. These measures include:

Digital Certificates

The WebPortfolio applet, the Custodial Integrator cabinet files, and the service website are authenticated by digital certificates from VeriSign™. These digital signatures confirm the authenticity of the application and the identity of the service with which data is exchanged.



Secure Connection - HTTPS

Connections to the service require HTTPS (HTTP over an encrypted SSL connection). Sessions on unencrypted connections are not allowed. The service website attempts to use “strong” (128-bit) encryption first, then falls back to “export” (56-bit or 40-bit) encryption if the user’s browser does not support strong encryption. This scheme makes the service compatible with whatever encryption policy a customer may require of its web site users, while also using the strongest measures possible to protect the communication.

Session Management

All service activities take place within an authenticated session (user must log in before being allowed to do anything). Sessions are closed automatically after a period of inactivity. No ByAllAccounts service or application uses “cookies” for tracking or session management.

Data Encryption

All sensitive data is transmitted and stored encrypted, even when communication is between components of the service itself. Values that need to be decrypted for use are encrypted using a strong two-way encryption algorithm. Values that do not need to be decrypted are encrypted using a strong one-way encryption algorithm and cannot be decrypted.

Decryption keys are maintained in a password-protected key store. The key store is not accessible from the machine(s) on which the database resides, nor is the key store present on any database back-up (where the data remains encrypted).

Application Features

WebPortfolio provides several security features, such as:

- **Financial Data Access Roles** – A hierarchy of roles and permissions defines who can access what financial data from within ByAllAccounts' products. Roles include: Advisor, Client, Consultant, and Administrator. These roles and permissions may be used not only to control who may edit information, but also to control who may see any of a client's personal information (account numbers, etc.)
- **Audit Logs and Notifications** – Use of any system administrative function (such as resetting a user's password) is recorded in a log file. These functions also send email to the affected user.
- **Investor Account Access** – When an advisor and client are working together, the service allows registration of accounts at remote financial services for which information is to be gathered without the advisor ever seeing or knowing the credentials (username/login ID and password/PIN). The client is directed to a secure web form where this information is supplied, encrypted and stored directly in our database. No one other than the client sees these credentials during this process.
- **Password Retrieval** – No product or service available from ByAllAccounts delivers or displays any password or PIN. It is not possible for a client, an advisor, an advisor's firm, or technical support personnel to "look up" a client's password – not even at the client's request – for access to WebPortfolio or for access to a particular financial service from which information is retrieved.

Employee Policies

ByAllAccounts employs a comprehensive set of policies and procedures that monitor and maintain a consistently high level of security. These policies and procedures include:

- Citizenship/Residency verification
- Social Security/Tax ID Number verification
- Education/Degree verification
- Periodic criminal background checks
- Periodic credit checks
- Password controls
- Explicit privacy and sensitive information handling agreement
- Security policy compliance performance review component

Privacy

The privacy of our clients' information as well as the users of our data gathering technology is paramount. ByAllAccounts' privacy policies as well as privacy statements have been designed specifically with this in mind.

ByAllAccounts' Privacy Statement

There is nothing more important to us than protecting the privacy of our customers and safeguarding their personal and financial information (also see Security Statement). This Privacy Statement explains our practices with respect to the collection and protection of that information and addresses the concerns regarding the disclosure of personal and other information to third parties.

For the sake of this document, "personal information" is defined as any and all of the information specific to an advisor, an advisor's client, or an individual investor that is submitted over the Internet or any other channel. This includes a person's name, address, phone number, email address as well as any financial service login ids, passwords, account numbers, and any other information supplied when registering an account with the WebPortfolio service. Custodial Integrator clients use the WebPortfolio service only for the user and account registration process, and in this respect are affected by this Privacy Statement.

What type of personal information will be collected?

During the user registration process, the following information is gathered:

- Name*
- Email Address*

*Occasionally, we may find it necessary to contact the user regarding account status and other matters relevant to the underlying service and/or the information collected. We will use the Name and Email Address associated with the account for this purpose; this name and address may be that of the advisor or that of the investor.

We may also send service related communications via email. This is entirely optional, and can be changed at any time from within the application.

What information is collected for on-line account access?

This is usually at least a login id (which may be a user name, customer number, account number, social security number, etc), a password/PIN, an account number or other unique account identifier, and – depending on the nature of the service - a social security or tax identification number. Some financial services may require additional login or account identification information, which will also be collected. Only information required to access

the financial service and to select the account(s) whose information is to be gathered is collected.

Are Cookies Used?

No, we do not use cookies of any type.

How Does a User Discontinue Service?

Use of the WebPortfolio service can be discontinued at any time via the service setup application. When the service is discontinued, all account information (current and historical) is deleted from our database.

Security Statement

We employ industry-leading technologies and policies to protect the confidentiality and privacy of each user's financial and personal data (also see Privacy Statement), and will continue to update our systems to stay at the forefront of security processes and technologies. The following steps have been taken to provide a completely secure experience for the client:

Our People

We require that any employee with access to our production systems or to our service's software pass both a criminal background check and a credit check before hiring. These checks are repeated on a regular periodic basis thereafter.

128-bit Secure Sockets Layer (SSL)

We use the industry standard SSL protocol currently used by leading financial service providers and banks, to encrypt and ensure the privacy of data as it moves between the user's browser and its web servers. We support symmetric 128-bit encryption for the maximum level of security supported by the latest Microsoft and Netscape browsers.

Physical Security

All personal user information is stored in an encrypted format in our database, and is transmitted in that encrypted format within the network. Our servers and database of user information are physically protected at a highly secure third-party site. This site is protected from outside access by a series of firewalls and a comprehensive suite of security products, and is internally monitored by security personnel and under surveillance twenty-four hours a day. Only a limited number of authorized personnel are granted access to the data center, and only after successfully passing multiple forms of positive personal identification verification.

Rest Assured



There is nothing more important to ByAllAccounts than protecting the privacy of its customers and safeguarding their personal and financial information.

[More Security Information :: Click Here](#)