Morningstar ByAllAccounts Service Security & Privacy Overview

Version 3.8

April 2018

10 State Street,
Woburn, MA 01801-6820
USA Tel: +1.781.376.0801 | Fax: +1.781.376.8040

byallaccounts.morningstar.com

OVERVIEW

Morningstar® ByAllAccounts® aggregation service data gathering technology captures and manages highly sensitive information, including:

- names
- email addresses
- login IDs
- passwords

Morningstar places great emphasis on safeguarding this information and maintaining a high level of security around it. The ByAllAccounts Service employs industry-leading technologies and policies to protect the confidentiality and privacy of each user's financial and personal data. Morningstar 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 ensured continuity of service, as well as the ByAllAccounts Service privacy policies.

SECURITY

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

- Network security
- Application security
- Encryption

The ByAllAccounts Service encrypts all personal user information whenever it is transmitted or stored.

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

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

Morningstar has a comprehensive Information Security Policy. In addition, Morningstar 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, Morningstar does not provide specific details regarding its security procedures and processes in this public document. Morningstar would be happy to discuss any questions or concerns our customers have 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 Service security processes.

Physical Security

The ByAllAccounts Service 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 by 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 Morningstar employees have access to the production machines.
- Access is logged.

Network Security

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

The ByAllAccounts Service 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.

The ByAllAccounts Service uses only state-of-the-art equipment from proven, mainstream vendors 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

The ByAllAccounts Service implements a number of security measures. These measures include:

- **Digital Certificates**
  The Custodial Integrator cabinet files, and the service website are authenticated by digital certificates from a trusted commercial vendor. 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 requires use of "strong" (128-bit). 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

The ByAllAccounts Service 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 the service. 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 the ByAllAccounts Service 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 the ByAllAccounts Service or for access to a particular financial service from which information is retrieved.

Security Breach

During an incident, the Incident Management and Response Team will start the analysis and recovery phase to direct triage, response, and recovery; provide technical support and expertise related to impact assessment, incident handling, and technical system management; report incidents to appropriate internal management teams and/or authorities as required; record incident details using Morningstar's standard incident report templates; and prepare external/internal communications and updates. The team will then use Morningstar's standard root cause analysis template to determine what controls or procedures can be put into place to prevent the incidents from reoccurring.

Business Continuity Plan

Morningstar provides business continuity, disaster recovery, and backup capabilities and facilities, through which Morningstar is able to perform its obligations to its clients, with minimal disruptions or delays. Morningstar maintains and exercises its Business Continuity Plan (BCP) once a year and it also revises its BCP to conform to new governmental regulations, if applicable.

Data Safeguards

Morningstar maintains data safeguards against the destruction, loss, or alteration of, or unauthorized disclosure of or access to client's data in its possession, including while in transport.

Employee Policies

Morningstar subjects employees to a comprehensive set of policies and procedures that monitor and maintain a consistently high level of security. These policies and procedures include:

- Identity and work authorization verification
- Social Security/Tax ID Number verification
- Education/Degree verification
- Criminal background checks prior to hire
- Explicit privacy and sensitive information handling agreement
- Security policy compliance performance review component
- Screening of personnel from sensitive communications and information

PRIVACY

The privacy of our clients' information as well as the users of our data gathering technology is paramount. The ByAllAccounts Service privacy policy as well as its privacy statement (shown below) have been designed specifically with this in mind.

PRIVACY STATEMENT - BYALLACCOUNTS SERVICE

There is nothing more important to us than protecting the privacy of our advisor clients and their customers and safeguarding the personal and financial information submitted to us on their behalf. This Privacy Statement explains our practices with respect to the collection and protection of that information via the ByAllAccounts Service 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 a natural person, whether an advisor, an advisor's customer, or an individual investor that is submitted to Morningstar via the ByAllAccounts Service. This information includes the individual's name, street address, phone number, email address, as well as any financial service login IDs, passwords, account numbers, and any other information tied to an identified or identifiable individual that is supplied to Morningstar as part of the ByAllAccounts Service. registration process, and in this respect are affected by this Privacy Statement.

What type of personal information will be collected during the registration process?

During the user registration process, the following information may be gathered:

- Name
- Email Address
- Street Address (if provided)
- Phone Number (if provided)

Occasionally, we may find it necessary to contact the user regarding account status and other matters relevant to the 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 advisor’s customer/investor.

What personal information is collected for on-line account access?

Personal information required to allow on-line access usually includes 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 system requirements of the financial institution (a.k.a., the Account Provider) maintaining the account(s) in question -- a social security or tax identification number. Some Account Providers may require additional login and/or account identification information in order for their customers to access the individual accounts maintained on their behalf. To the extent necessary, this information will also be collected. Morningstar will use all reasonable efforts to only collect that personal information necessary to enable it to provide the ByAllAccounts Service.

Use of personal information

EXCEPT WHERE OTHERWISE AUTHORIZED BY YOU OR WHERE REQUIRED TO COMPLY WITH LAW OR ANY COURT/GOVERNMENT ORDER, Morningstar will not sell, exchange, or release any of your personal information to a third party (including the vendor whose website was used to access the ByAllAccounts Service).

Accuracy of personal information

You are responsible for ensuring that any personal information entered or reviewed by you, including all on-line account access information in the ByAllAccounts Service, is accurate and up-to-date.

Your consent

By using the ByAllAccounts Service, you consent to the collection and use of your personal information, as described in this Privacy Statement and the Morningstar® ByAllAccounts® User Agreement. The ByAllAccounts Service systems are not currently configured to handle "Do Not Track" requests.

Are Cookies Used?

No, Morningstar does not use cookies as part of the ByAllAccounts Service.

How Does a User Discontinue Service?

Use of the ByAllAccounts Service can be discontinued at any time via the Service setup application. When the ByAllAccounts Service is discontinued, all account information (current and historical) is deleted from our database on the timeframe set forth herein.

Changes to the Privacy Statement

Morningstar reserves the right to change this Privacy Statement at any time by distributing and/or posting a new Privacy Statement without notice. We encourage you to review our Privacy Statement periodically so that you are aware of any changes to it.

Any questions or issues around this Privacy Statement may be directed via email to: byallaccounts-support@morningstar.com or by calling the support number at 866-856-4951.