MORNINGSTAR Wealth

Morningstar ByAllAccounts Service
Privacy & Security Overview

Version 3.9

April 2, 2024

22 West Washington Street
Chicago IL 60602 USA

www.morningstar.com/products/byallaccounts

INTRODUCTION

Morningstar® ByAllAccounts® financial data aggregation platform accesses, stores, and processes highly sensitive information of our customers and their clients, including:

- names
- email addresses
- login IDs
- passwords and tokens
- trading behaviors and positions

Morningstar places great emphasis on safeguarding this information and maintaining a high level of security throughout the data lifecycle. The ByAllAccounts Service employs financial industry-leading technologies and policies to protect the confidentiality and integrity of each user's financial and personal data, as well as the privacy of each user on our platform. Morningstar regularly updates its systems to stay at the forefront of security, privacy, and continuity protection.

This document describes the security and privacy measures of our platform and services, including physical protection of information, disaster recovery, and continuity of service, as well as the ByAllAccounts Service privacy policies.

Morningstar® ByAllAccounts Privacy Statement

Last updated: April 2, 2024

Overview

ByAllAccounts understands that it's important to our customers that we keep their personal and financial information safe. This statement outlines our commitment to protecting the privacy and security of the data you entrust to us. This statement applies to the personal information you or your financial advisor give us when you use our services. Please note, however, that we don't control how you or your advisor use or share your information after you retrieve it from us. This privacy statement is intended to supplement, rather than supersede, Morningstar's General Privacy Statement.

This privacy statement applies to ByAllAccounts users in the United States.

Types of information we collect

We'll only collect your information if you directly provide it to us, including through information collected when you use or services or sites, or if you consent to a third-party providing it to us.

When you create an account or subscribe to ByAllAccounts products, you may give us basic information about you, including your:

- Name
- Email address
- Username and password
- Street address

- Phone number
- Financial advisor's information, including name and contact information

When you use ByAllAccounts to collect information from your third-party accounts (for example, you may ask us to collect your information from an investment account), you will give us personal information related to that account, including your:

- Username and password for that account
- Account numbers
- Transaction or investment information

We may also collect certain usage information when you use our sites, including Internet Protocol (IP) addresses, log files, browser type, and other related information.

How we use your information

- We collect your information so that you can use it in other financial applications, such as Morningstar Office, Morningstar Advisor Workstation, or other third-party financial planning and reporting applications that you choose.
- We use the information you give us to retrieve your data from the third-party accounts you authorize us to access.
- We use your information to contact you. We may contact you to support your account or to provide you with notices related to your services. In limited circumstances, we may contact you for marketing purposes.
- We use information from our website, such as IP address information, to improve the services we offer.
- We use and share anonymized customer information for research purposes and to improve our products. When we share your information for these purposes, we always remove any information that can identify you.
- We may share your information when necessary to comply with legal obligations.
- Our service providers who work on our behalf may have access to your information. These service providers only perform services related to the purposes described in this statement.

We won't sell your information and we won't share your information with a third-party unless we have your consent or in the limited cases we describe above.

How we protect your information

The security of your information is our priority.

- We maintain a comprehensive information security program that requires that we use physical, technical, and procedural safeguards intended to keep your information safe.
- We use encryption when we store your information (encryption at rest) and when we transfer your information (encryption in transit).

We've also designed features that help you control the security of your information:

- We allow you to control what information your advisor can see, edit, or manage.
- We keep logs of all changes that we make to your account (such as resetting your password) and we send you an email when we make a change.

- We do not store your password in open text, so it is not possible for your advisor or our staff to look up your password to access your ByAllAccounts or third-party accounts.

If you have additional questions about how we keep your information safe, please Contact Us.

How do we store your information?

We only store our customers' information in the United States.

We'll retain your information for as long as necessary to fulfill the purpose for which it was collected or to comply with legal, regulatory, or internal policy requirements. After you deactivate your account, we'll delete your information within ninety (90) days, unless you instruct us otherwise or unless we have another legal reason to retain the information.

Your rights

You have the right to access, control, or delete your personal information that we store or to ask us to stop collecting information from your third-party accounts. You can also ask us to provide the general types of information we collect about our customers, who we collect it from, how we use or share it, and our business purpose for collecting, using, or sharing this information.

If you have an account with us, you can manage your information from within your ByAllAccounts profile. If you don't have a profile (for example, your advisor may have given us your personal information in order to provide you services) or if you are otherwise unable to access, control, or delete your information from within your profile, please visit our Privacy Center or Contact Us for help.

We won't discriminate against our customers who choose to exercise their rights to access, control, or delete their personal information. Some of our products and services, however, may require your personal information. If you choose not to provide your personal information, you may not be able to use those products or services.

How does a user deactivate their account?

You can deactivate your ByAllAccounts account at any time through the ByAllAccounts application. When you deactivate your ByAllAccounts account, we will delete all of your account information within ninety (90) days, unless you instruct us differently or unless we have another legal reason to retain the information. You may also submit a request to delete your account or information through the Privacy Center and you may Contact Us for help.

Consumer Rights and Disclosures

Some state privacy regulations require that we list the categories of our customers' personal information that we've sold or disclosed for business purposes in the last twelve (12) months.

- ***Sales***: In the last twelve (12) months, we haven't sold our customers' information.
- ***Disclosures***: In the last twelve (12) months, we've only disclosed customer information as directed by our customers. We've disclosed personal identifiers (for example, name and account information) and commercial information (for example, transaction or investment-related information) to financial service providers and to customers and their agents directly.

Some states give consumers the right to request that a company not sell their personal information. If you reside in a state that gives their residents this right and wish to exercise it, please visit our Privacy Center, Contact Us, or call us toll-free at +1 (888) 293-8609.

Cookies

We use cookies for authentication and application usage analytics purposes. These cookies allow you to sign in to our site. If you would like to learn more about how we use cookies in general, please visit our Cookie Policy.

Children's Privacy

We don't separately identify, or collect, any information that is specific to children.

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.

How we revise this statement

Our business frequently changes, and we may need to update this statement to reflect those changes. When we make changes to this privacy statement, we'll revise the "last updated" date at the top of this page. If we make material changes to this statement, we'll notify you directly as required by law.

Contact us

If you have a concern, complaint, or question about how we handle your personal information, please Contact Us, call us toll-free at +1 (888) 293-8609, or write us at the following mailing address:

Morningstar, Inc.
22 W. Washington St.
Chicago, IL 60602
Attn: Chief Privacy Officer

Security Statement

Last updated: April 2, 2024

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

- Network security
- Application security
- Encryption

In particular:

- ✓ 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 public forums. Morningstar would be happy to discuss any questions or concerns our customers have regarding its security, resilience, or privacy programs.

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

Physical Security

The ByAllAccounts Service runs on servers and databases of user information that are physically protected at a highly secure site. The physical premises are internally monitored twenty-four hours a day by security staff. 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 and reviewed on a quarterly basis.

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 HTTPS (443). All other ports have been closed down as part of the system design.

The ByAllAccounts Service uses only production grade equipment from proven, mainstream vendors to provide secure hardware environments. Additional network-level security includes anti-spoofing, secure DNS, and anti-virus via 24x7 detection and monitoring. Reasonable log retention 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" (256-bit) 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

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 its employees to a comprehensive background check to maintain a consistently high level of security. In addition, employees must agree to a comprehensive set of policies designed to maintain security. The background checks and policies 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