

MASSACHUSETTS INFORMATION SECURITY AND DATA HANDLING DISCLOSURE

Monorail Securities LLC — for Massachusetts residents — Rev. September 2026

This disclosure accompanies our privacy notice. It describes how we protect, handle, and dispose of the personal information of Massachusetts residents, and what we do if that information is compromised. It is not a consent form and there is nothing for you to sign or return.

Your choices are handled in the privacy notice, not here

We do not disclose your identity, affairs, or investments to any outside company that is not servicing your account, except as our privacy notice describes. If an investment adviser referred you to us, we share the limited information listed in that notice with that adviser, and you may stop that sharing at any time — using the opt-out election form, the Privacy Choices screen in the Monorail app, or any of the methods at the end of this disclosure. Stopping it costs you nothing: we will not deny you any product or service, change your fees, or treat you differently.

Our written information security program

We maintain a comprehensive written information security program covering the personal information of Massachusetts residents, as 201 CMR 17.00 requires and as Regulation S-P separately requires. Our Chief Compliance Officer is responsible for maintaining it. The program is reviewed at least annually, and whenever there is a material change in our business practices that could affect the security of personal information.

What we do to protect your information

Access controls. We limit access to your personal information to the employees and service providers who need it to do their work, and we remove access promptly when someone leaves or changes roles. Accounts are individually assigned, and access is blocked after repeated failed login attempts.

Encryption. We encrypt your personal information when it travels across public networks and when it is sent wirelessly, and we encrypt it on laptops and other portable devices and media.

System protection. We use firewalls, current security patches, and malware protection with regularly updated definitions on the systems that hold or transmit your personal information, and we monitor those systems for unauthorized access and use.

Physical safeguards. Records containing personal information are kept in secured files and secured buildings, and access to those areas is restricted.

People. We train the people who handle your information on our security program and we discipline violations of it.

Service providers. Before we give a service provider access to your personal information, we

take reasonable steps to confirm it can protect that information, and we require it by contract to maintain safeguards consistent with 201 CMR 17.00.

What we collect and how long we keep it

The categories of personal information we collect are listed in our privacy notice and include your Social Security number and date of birth, account balances and transactions, assets and investment experience, risk tolerance and investment objectives, contact information, and — for app users — device and login information. We keep your records for as long as you are our customer and afterwards for the period our books-and-records obligations require, currently five years after the account is closed. We do not keep personal information longer than we have a business or legal reason to.

How we dispose of your information

When we no longer need a record containing your personal information, we destroy it so that it cannot be read or reconstructed. Paper records are redacted, burned, pulverized, or shredded. Electronic media are destroyed or erased so that the information cannot be practicably read or reconstructed. We require our service providers to do the same.

If your information is compromised

If we know or have reason to know that your personal information has been acquired or used by an unauthorized person, or that unauthorized access has created a substantial risk of identity theft or fraud, we will notify you as soon as practicable and without unreasonable delay, and we will notify the Massachusetts Attorney General and the Office of Consumer Affairs and Business Regulation. Our notice to you will tell you about your right to obtain a police report, how to request a security freeze and what information you must provide, and any fees a consumer reporting agency may charge; Massachusetts law does not permit us to describe the nature of the incident or the number of residents affected in that notice. Separately, where Regulation S-P applies we will notify you within thirty days.

Questions, or to change your privacy choices

Mail: Monorail Securities LLC, Attn: Chief Compliance Officer, 3322 Bee Ridge Rd., Sarasota, FL 34239

Email: privacy@monorail.com | Phone: 941-925-2121 | Or use the Privacy Choices screen in the Monorail app.