Notice of Privacy Policy

Revised March 18, 2026

FACTS	**WHAT DOES MayTech Global Investments, LLC ("MayTech") DO WITH YOUR PERSONAL INFORMATION?**
WHY?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
WHAT?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social security number ▪ Income ▪ Assets ▪ Risk tolerance ▪ Birth date ▪ Tax identification numbers • Bank account numbers • Investment account numbers ▪ Wire transfer instructions ▪ Transaction history When you are no longer our customer, we continue to share information about you as described in this notice.
HOW?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons MayTech chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does MayTech Share?	Can you limit this sharing?
For our everyday business purposes - such as to process your transactions, maintain your accounts(s) or respond to court orders and legal investigations.	Yes	No
For our marketing purposes - to offer our products and services to you	No	We don't share
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes - information about your transactions and experiences	No	We don't share
For our affiliates' everyday business purposes - information about your creditworthiness	No	We don't share
For our affiliates to market to you	No	We don't share
For nonaffiliates to market to you	No	We don't share

Questions?	Call Tibor Nemes at 212-899-2735

MAYTECH
GLOBAL INVESTMENTS

Notice of Privacy Policy (Cont'd)

Page 2

Who we are	▪ *MayTech is a Registered Investment Advisor established in 2017.*

What we do	
How does MayTech protect my personal information?	To protect your personal information from unauthorized access and use, MayTech implements a comprehensive information security program that includes: (i) Administrative safeguards — written information security policies and procedures, employee training, vendor oversight, and periodic risk assessments; (ii) Technical safeguards — encryption of sensitive data in transit and at rest, multi-factor authentication, access controls, and intrusion detection systems; and (iii) Physical safeguards — secured office facilities, locked file storage, and controlled access to systems. Our safeguards program is reviewed and updated at least annually, and the status of the program is reported to senior management. In the event of a security incident, we will follow our Incident Response Program as described below.
How does MayTech collect my personal information?	We collect your personal information, for example, when you ▪ Enter into an investment advisory contract ▪ Seek financial advice ▪ Make deposits or withdrawals from your account ▪ Tell us about your investment or retirement portfolio ▪ Give us your employment history We also collect your personal information from others, such as your custodian bank.
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes—information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing.
How do I opt out?	MayTech does not share your personal information with nonaffiliates for marketing purposes. If our sharing practices change in the future, we will notify you and provide opt-out instructions. To exercise any opt-out rights, contact: Tibor Nemes at 212-899-2735 or tibor.nemes@maytechglobal.com.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies.

Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies.
Joint Marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you.
Nonpublic Personal Information (NPI)	Any information that a consumer provides to obtain a financial product or service, results from a transaction, or is otherwise obtained in connection with providing a financial product or service — that is not publicly available.
Sensitive Customer Information	A subset of NPI including Social Security numbers, driver's license numbers, financial account numbers, credit/debit card numbers, and biometric data, as defined under 17 CFR §248.30. (★ Added per Reg S-P 2024 amendments)

Reg S-P Amendments

A. Incident Response Program

MayTech maintains a written Incident Response Program ("IRP") designed to detect, respond to, and recover from unauthorized access to or use of customer information. The IRP includes:

1. Detection & Assessment. Procedures for promptly identifying and assessing actual or potential unauthorized access to sensitive customer information, including monitoring of access logs, anomaly detection, and regular vulnerability assessments.

2. Containment & Investigation. Steps to contain the security incident, preserve evidence, and investigate the scope and cause, including engagement of qualified cybersecurity professionals as appropriate.

3. Remediation. Procedures to remediate identified vulnerabilities, restore affected systems, and prevent recurrence, including patching, credential resets, and enhanced access controls.

4. Internal Reporting. The IRP is reviewed by senior management at least annually. A written report documenting incidents, investigations, and program status is provided to the Chief Compliance Officer no less than annually.

5. Recordkeeping. MayTech retains written records of all detected security incidents, investigations, determinations regarding notification obligations, and any notifications sent to customers for not less than five (5) years.

B. Customer Notification — Data Breach

Your Right to Be Notified. In the event of a security breach involving unauthorized access to or use of your Sensitive Customer Information, MayTech will notify you as soon as reasonably practicable, and in no event later than **30 days** after MayTech determines that a breach has occurred or is reasonably likely to have occurred.

The notification will be provided by email to your registered email address, or by written notice to your address of record, and will include:

• A description of the incident and the type of information involved

• The approximate date(s) of the unauthorized access or use

• Contact information for MayTech's Chief Compliance Officer

• A description of steps MayTech has taken or will take to address the breach

• Recommended protective actions you may take (e.g., credit monitoring, fraud alerts)

• Information about available resources, including the FTC's identity theft website (identitytheft.gov)

Exception. Notification may be delayed beyond 30 days only if a law enforcement agency determines in writing that notification would impede a criminal investigation.

C. Service Provider and Vendor Oversight

MayTech requires that all service providers and vendors that receive, maintain, process, or otherwise have access to customer information enter into written agreements that include contractual obligations to:

• Implement and maintain appropriate administrative, technical, and physical safeguards to protect customer information;

• Notify MayTech promptly — and in no event later than **72 hours** — upon becoming aware of any actual or suspected unauthorized access to customer information in the vendor's custody or control;

• Cooperate with MayTech in investigating and mitigating any security incidents; and

• Delete or return customer information upon termination of the service relationship.

MayTech conducts periodic due diligence of its service providers' information security practices and monitors for compliance with these contractual requirements.

D. Disposal of Customer Information

MayTech takes reasonable steps to dispose of customer information in a manner that protects against unauthorized access or use. Disposal methods include: secure shredding of physical records; secure deletion (degaussing or overwriting) of electronic records; and destruction or return of information held by third-party service providers upon termination of the service relationship. Records are retained for the minimum period required by applicable law, then disposed of in accordance with this policy.

E. Annual Privacy Notice

MayTech is required to provide you with a notice of its privacy policies and practices each year as long as you maintain a customer relationship with us. Consistent with the FAST Act exception under 17 CFR §248.5(e), MayTech may satisfy the annual notice requirement by making this Notice continuously available on its website at www.maytechglobal.com, provided that MayTech: (a) does not share nonpublic personal information other than as permitted under applicable exceptions; and (b) has not changed its policies and practices from those disclosed in the most recent notice previously delivered. MayTech will deliver a revised notice promptly whenever a material change to its privacy practices occurs.

F. State Privacy Laws

Depending on your state of residence, you may have additional privacy rights under applicable state law. For example, residents of California, Colorado, Virginia, Connecticut, Utah, and other states with comprehensive privacy statutes may have rights to access, correct, delete, or opt out of the sale or sharing of their personal information. To the extent state law provides additional protections or rights beyond those described in this Notice, MayTech will comply with applicable state requirements. Please contact MayTech's Chief Compliance Officer with any state-law privacy inquiries.