



Protecting Data. Preventing Fraud.

THE ACCOUNT PROTECTION PROGRAM

Safeguarding your employees' security and privacy is among our highest priorities. With sophisticated systems in place, we continually monitor and assess plan and participant account activity.

While we work hard to help ensure account security, you and your employees also play an important role. Under the new Account Protection Program, T. Rowe Price will cover account losses caused by unauthorized activity if both the employee and employer take a few simple, proactive steps. It's all part of our firmwide commitment to security and privacy.

PROTECTING IN ACTION

Our enterprise-wide security strategy protects account holders with a combination of technology, policies, and processes.



Governance

A security strategy informed by regular briefings and an established business continuity plan



People

Vetting of associates, who are also trained and supported in security awareness and privacy incident prevention



Process

Ongoing risk assessment, management, and testing throughout the firm



Technology

Advanced network and data protection, identity and access management, and cybersecurity data analysis



Vigilance/ Monitoring

Continuous monitoring of plan and account activity

WORKING TOGETHER FOR MORE SECURE DATA

Employees are automatically protected by the Account Protection Program if you and your employees take the steps below. For more information, see the **Account Protection Program** page on the Workplace Retirement site.



Plan Sponsors

Maintain access to T. Rowe Price systems

- Monitor, update, and remove, if applicable, user access in a timely manner, using permissions to enable only the functions each user needs
- Leverage security provisions to minimize visibility of confidential information such as Social Security numbers

Use secure methods to send files and download data

- Always send files using secure methods approved by T. Rowe Price
- Leverage on-demand reporting to access data
- Limit downloading from systems

Take precautions to protect assets

- Establish a robust plan for monitoring threats and maintaining and securing assets
- Train and support employees in protecting assets

Employ effective controls when using suppliers

Maintain a supplier management program with onboarding and ongoing monitoring to ensure supplier compliance with standards for data protection



Participants

Must follow these four security best practices:

- Establish a T. Rowe Price online account and Multi-factor Authentication
- Maintain an up-to-date mailing address, email address and phone number(s) on your T. Rowe Price account
- Review T. Rowe Price account statements, confirmations, and correspondence within 30 days after that information is posted to your online account or delivered to you by mail
- Contact T. Rowe Price immediately at **1-800-922-9945** if you suspect any unauthorized account activity, notice errors or discrepancies in your account, or if you are not receiving your T. Rowe Price account statements.

Plan sponsors and participants should **contact us immediately** if they suspect a potential breach or fraudulent activity. The Account Protection Program will not apply if the four security best practices outlined above are not followed. All reported concerns will be thoroughly investigated. T. Rowe Price will determine the applicability of the Account Protection Program and the type and amount of any reimbursement by reviewing the facts and circumstances associated with each reported event.

To learn more, contact your T. Rowe Price representative.