Cottage Street | Advisors

9 Cottage Street
P.O. Box 249
Marion, MA 02738

MARCH 2025: PRIVACY POLICY NOTICE AND PERSONAL INFORMATION SECURITY

Your privacy is important to us. To better protect your privacy, we provide this notice explaining what Cottage Street Advisors, LLC does with your personal and financial information. Federal law gives consumers the right to limit some but not all sharing of this information. 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.

The types of personal information we collect and share depends on the products and services that you have with us. The information that we typically collect typically includes: Social Security number, employment status and income, account balances and assets transaction history. All financial companies need to share customers' personal information to perform their services and run their everyday business.

We will share your personal information to conduct business and help manage your account. Specifically:

- To process your transactions, invest your assets, maintain your account(s), respond to court orders and legal investigations.

- To provide appropriate information that is required or requested for tax purposes, tax planning or estate planning, or asset protection planning purposes.

You are allowed to limit this sharing.

To protect your personal information from unauthorized access and use, we store as little of your personally identifiable information as possible and use security measures that comply with federal law. These measures include computer safeguards (such as password protection or encryption) and restricting access to physical files (such as locked cabinets and building access).

We collect your personal information, for example, when you:

- Open an account
- Deposit money
- Seek advice about your investments or tax matters
- Enter into an investment advisory contract
- Tell us about your investment or retirement portfolio or earnings

We do not share information with Affiliates, Non-Affiliates or for Joint Marketing purposes.

Affiliates include companies related by common ownership and/or control. They can be financial and non-financial companies. Non-affiliates include accountants, attorneys and other business professionals. Joint marketing is typically a formal agreement between non-affiliated financial companies that together market financial products or service to you**.** Furthermore, we will not discuss your personal data, circumstances or account balances with other individuals unless instructed to do so by you.

Basically, we won't disclose your personal information to anyone unless you ask or authorize us to do so. We will rely on your instruction before we share your data or information with your other service providers, such as your accountant or attorney and even other family members. If you have a joint account, your choices will apply to everyone on your account – unless you tell us otherwise.

INFORMATION THAT WE WON'T ASK FOR:

We will **never** ask you for ID or passwords to any account. We have the access we need to view your account information and trade on your behalf under our advisor arrangement.

Unless we are working together on a request that you initiate, **we will also not ask you for any bank account or ACH information**. We are not authorized to move money on your behalf but will certainly help you complete the paperwork to move money or set up ongoing transfers at your request.

In general, our requests to you for information are associated with administrative or services requests that you initiate, such as an asset transfer or mailing address change.

If you are ever unsure of any request for information from us via e-mail, text or voice-mail, please call the office to verify the authenticity.

Should you have any questions or concerns about these privacy policies, please call Jason Haviland, Chief Compliance Officer, at 508-748-0709.

PERSONAL INFORMATION AND FRAUD:

The Security of your Personal Information is Important to Us

In an ongoing effort to keep our clients informed and aware of identity protection measures and cybersecurity guidelines, we are providing this circular as a helpful reminder of the following information to help you keep your information secure.

We will ***NEVER***:

- ✓ Ask for Social Security Number (SSN) or other personally identifiable information via email
- ✓ Ask for login credentials or passwords
- ✓ Accept trade instructions or fund transfer requests by email or voicemail – these must be verbally confirmed EVERY TIME
- ✓ Ask for payment or account details via email (unless through encrypted service or eSignature form)
- ✓ Send you an email requesting that you "verify" any personal information (unless through encrypted service or eSignature form)

Use the Tools You Have to Protect Your Identity and Accounts

- ✓ Monitor your accounts online; be aware of your balances and holdings
- ✓ Be alert to "phishing" scams which seek to gain access to your personal information
- ✓ Protect your login IDs and passwords; use a combination of letters, numbers and special characters for your passwords and change them at least every 90 days; do not carry them on you/in your wallet
- ✓ Do not give your SSN or other personal information about yourself to anyone you do not know
- ✓ Order copies of your credit report once a year to ensure accuracy
- ✓ Choose to do business with companies you know are reputable, particularly online
- ✓ When conducting business online, make sure it is a secure transaction (look for **HTTPS** in the address)
- ✓ When using social media sites, NEVER publish personal information including telephone numbers, Social Security number, date of birth, email addresses, physical address, mother's maiden name or other information that may be sensitive information to fraudsters or hints to passwords
- ✓ Do not open email from unknown sources and use virus detection software

What to Do if You Believe You are a Victim of Fraud

- ✓ Contact us immediately if you know or suspect your identity has been stolen or your account has been compromised.
- ✓ File a police report and contact the three major credit reporting companies; the fraud unit numbers are:

  Transunion – (800) 680-7289
  Experian – (888) 397-3742
  Equifax – (800) 525-6285

- ✓ Keep records of your communications with authorities, including names, contact numbers and dates and times of the calls

How Not to Get Hooked by a "Phishing" Scam

Phishing is a high-tech scam that uses spam emails or pop-up messages to deceive you into disclosing investment account numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization with which you already do business, such as your Internet Service Provider, investment adviser, bank, online payment service, or even a government agency. The message typically states that you must "update" or "validate" your account information, and it may additionally allude to dire consequences in the event you fail to respond (i.e., the closure or suspension of your account). The message then redirects you to a fraudulent website designed to look like a legitimate site for the organization; however, it is not. The purpose of the fraudulent site is to trick you into divulging your personal information so the operators can steal your identity, run up bills or commit crimes in your name.

The FTC, the nation's consumer protection agency, suggests these tips to help you avoid getting hooked by a phishing scam:

- ✓ If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct website address. NEVER cut and paste the link in the message.
- ✓ Do NOT email personal or financial information. Email is NOT a secure method of transmitting personal information. Protect your personal information at all costs and only divulge in person or by phone to an individual known or verified by you.
- ✓ Review credit card and bank account statements routinely to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- ✓ Use anti-virus and anti-malware software and keep your programs up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Antivirus software and a firewall can protect you from inadvertently accepting such unwanted files. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It is especially important to run a firewall if you have a broadband connection. Always install routine updates to ensure your software is current to evolving schemes.
- ✓ Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.
- ✓ Report suspicious activity to the FTC. If you receive an email phishing for information, forward it to www.ftccomplaintassistant.gov. If you believe you have been scammed, file a complaint at www.ftc.gov, and then visit the FTC's Identity Theft website at www.ftc.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam. The FTC works on behalf of the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, (877)-FTC-HELP ((877)-382-4357); TTY: (866)-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.