Mariner Wealth Advisors, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

MARINER

1 1 5 **********AUTO**ALL FOR AADC 303

May 29, 2026

Re: Notice of Security Incident

Dear ,

I am writing to inform you of a recent security incident at Mariner Wealth Advisors, LLC ("Mariner", "we," or "us") involving three (3) of our associates' cloud applications that may have resulted in unauthorized access to some of your personal information.

Please note that this incident was isolated to these three (3) associates and their specific cloud applications. **Financial accounts, investment accounts, and other client accounts are stored on entirely separate systems at entirely separate entities that were unaffected by this incident.** A number of controls are in place to detect and prevent suspicious activity within those systems, and they remain safe and secure.

What Happened? Mariner initially detected suspicious activity on November 24, 2025, tied to Mariner users' cloud applications. Mariner immediately initiated its incident response plan and began containment measures. Those accounts were immediately isolated, secured, and analyzed to confirm containment. We have been communicating with federal law enforcement and regulatory authorities. Mariner's investigation performed alongside third-party experts has determined that a criminal third party accessed the accounts and downloaded certain files during that time. A thorough review of the files involved determined some of the files contained your personally identifiable or non-public personal information.

What Information Was Involved? Files containing your individual name, along with information needed to service your account such as your account number(s), date of birth, and/or social security number or other government ID number. We have no evidence that any files, including those containing your personal information, have been misused as a result of this incident. Mariner has engaged third-party researchers to monitor websites, forums and other online sources for signs of data misuse, and none has been found.

What We Are Doing. We are committed to protecting the personal information we maintain here at Mariner. The referenced cloud applications have been secured. We will continue to emphasize cybersecurity awareness in our employee training materials and are working with our external advisors to fortify our cybersecurity defenses.

What You Can Do. We have no indication that any personal information has been misused as result of this incident, nor do we expect this to occur. Nevertheless, we have enclosed instructions on how to enroll in a complimentary credit monitoring service for the next twelve (12) months. If you are interested in this service, you can enroll online or by phone. Enrollment in this service is completely free and will not

impact your credit score. We are also enclosing several information resources to learn more about steps that can be taken to address any concerns you may have about identity theft or fraud.

For More Information. If you have any questions about this incident, or to activate your complimentary credit monitoring service, please reach out to our dedicated support team at from 8:00 am to 8:00 pm EST Monday through Friday (excluding major U.S. holidays). For any other questions please contact your investment advisor.

Sincerely,

Mariner

DETAILS REGARDING YOUR CYBERSCOUT MEMBERSHIP

We are offering you complimentary access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To activate your membership and start monitoring your credit, please follow the steps below:

- Ensure that you **enroll within 90 days from the date of this letter** (Your code will not work after this date.)
- Visit the Cyberscout website to enroll: **https://bfs.cyberscout.com/activate**
- Provide your unique code: .

The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. **Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.**

ADDITIONAL IMPORTANT INFORMATION

1. Review Your Credit Reports. We encourage you to regularly review your account statements and credit reports for any unfamiliar or suspicious activity. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which that account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to the proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

Additionally, federal law allows you to obtain one free credit report every 12 months from each of the three nationwide credit reporting agencies. You may request your free annual credit report by visiting www.annualcreditreport.com, calling (877) 322-8228, or completing the Annual Credit Report Request Form available on the FTC's website at www.ftc.gov and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Free annual credit reports are available only through these official methods.

If you notice information on your credit report that you do not recognize or believe to be inaccurate, you should contact the applicable credit reporting agency using the contact information provided in the report. Promptly reporting errors or potentially fraudulent activity allows the credit bureau to investigate and, if appropriate, correct the information. If you identify accounts or transactions that you did not authorize, notify the credit reporting agency immediately by phone and in writing.

2. Consider Placing a Fraud Alert. You may place a fraud alert on your credit file by contacting one of the three major credit reporting agencies by phone or through Experian's or Equifax's websites. A fraud alert advises lenders to take additional steps to verify your identity before opening new accounts or making changes to existing accounts. Please note that fraud alerts may result in delays if you later apply for credit.

You may obtain additional information or place a fraud alert by contacting the credit bureaus listed below:

Equifax https://www.equifax.com/personal/credit-report-services/ 1-888-298-0045 Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian https://www.experian.com/help/ 1-888-397-3742 Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion https://www.transunion.com/credit-help 1-800-916-8800 TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

It is only necessary to contact one of these bureaus and use only one of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You should receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

3. Place Security Freezes. A security freeze restricts access to your credit report, helping prevent identity thieves from opening new accounts or obtaining credit in your name. Federal and state laws prohibit credit bureaus from charging fees to place, temporarily lift, or remove a security freeze. Please be aware that while a freeze is in place, you may be unable to obtain new credit, loans, or credit cards unless you lift or remove the freeze.

To request a security freeze, you must contact each of the three credit reporting agencies listed above and provide the following information: (1) your full name; (2) Social Security number; (3) date of birth; (4) addresses where you have lived during the past two years; (5) documentation showing your current address, such as a utility or telephone bill; (6) a copy of a government-issued photo identification; and (7) if applicable, documentation of identity theft, such as a police report or complaint to law enforcement.

If you submit your request by phone or secure electronic means, the credit bureaus must place the security freeze within one business day of receiving your request. Requests submitted by mail must be processed within three business days of receipt. Each bureau will send written confirmation of the freeze within five business days, along with instructions on how to lift or remove the freeze if needed. There is no charge to place a security freeze.

4. Request an IP PIN from the IRS. Although the IRS is capable of identifying suspicious tax returns, taxpayers may choose to take proactive steps to prevent fraud, including obtaining an Identity Protection PIN (IP PIN) from the IRS. The IP PIN is a 6-digit number that, when active, will be required to file a tax return using the taxpayer's SSN or ITIN. To request an IP PIN, visit https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

In addition, taxpayers may opt in to ID.me, an identity verification service that requires a photo ID or live video session before logging in to submit a tax return online.

Finally, taxpayers may submit IRS Form 14039, Identity Theft Affidavit online if they received IRS correspondence indicating they might be a victim of tax-related identity theft or if their e-file tax return was rejected as a duplicate. After submitting the form, the IRS will refer the taxpayer's case to the Identity Theft Victim Assistance organization to investigate the case, remove fraudulent returns, and process the correct return and refund.

5. Monitor Your Financial Accounts. We recommend that you routinely review your bank, credit card, and other financial account statements for any unauthorized or unusual activity. If you identify transactions or activity that appear suspicious, promptly notify the relevant financial institution or service provider.

6. Learn More About Identity Protection Resources. You can further educate yourself about identity theft, fraud alerts, security freezes, and additional steps you can take to protect your personal information by contacting the national consumer reporting agencies, your state Attorney General's office, or the Federal Trade Commission ("FTC"). The FTC can be contacted at 600 Pennsylvania Avenue NW, Washington, DC 20580; online at www.identitytheft.gov; by phone at 1-877-ID-THEFT (1-877-438-4338); or via TTY at 866-653-4261. The FTC also encourages individuals who believe their information has been misused to submit a complaint.

This notice was not delayed by law enforcement.

District of Columbia Residents: You can obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, https://oag.dc.gov/.

Iowa Residents: You can report suspected identity theft to law enforcement, the FTC, or to the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, https://www.iowaattorneygeneral.gov/.

Maryland Residents: You can obtain additional information about identity theft prevention and protection from the Maryland Attorney General, Identity Theft Unit at: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, 1-866-366-8343 or (410) 576-6491, https://www.marylandattorneygeneral.gov.

Massachusetts Residents: You have a right to file a police report and obtain a copy of your records. You can obtain additional information about identity theft prevention and protection from the Office of Consumer Affairs and Business Regulation, 501 Boylston Street, Suite 5100, Boston, MA 02116, (617) 973-8787, https://www.mass.gov/service-details/identity-theft.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General, The Capitol, State Street and Washington Avenue, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/.

North Carolina Residents: You can obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free within North Carolina) or (919) 716-6000, https://ncdoj.gov/.

Oregon Residents: You can report suspected identity theft to law enforcement, the FTC, or the Oregon Office of the Attorney General at: Oregon Department of Justice, 1162 Court St NE, Salem, OR 97301, 1-800-850-0228, https://www.doj.state.or.us/.

Rhode Island Residents: You can obtain additional information about identity theft prevention and protection from the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, https://riag.ri.gov/. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. There are approximately 12 Rhode Island residents that may be impacted by this event.