PIERCE ATWOOD LLP

PETER J. GUFFIN

Merrill's Wharf
254 Commercial Street
Portland, ME 04101

pierceatwood.com

Admitted in: MA, ME

July 7, 2023

VIA EMAIL

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Data Security Incident

Dear Attorney General Formella,

We are writing on behalf of our client, Pear Tree Advisors, Inc. ("PTA"), which serves as transfer agent for Pear Tree Funds. PTA has asked us to provide your office with information regarding a data security incident that impacted the personal information of 100 residents of New Hampshire.

PTA uses an investor management system provided by a company called Envision Financial Systems, Inc. ("Envision") to assist with certain functions PTA provides to Pear Tree Funds. Envision stores Pear Tree Funds' shareholder data in a private cloud environment managed by a subcontractor, Integrated Systems Corporation ("ISCorp"). On May 31, 2023, ISCorp became aware of a vulnerability in a widely used file transfer software application that ISCorp uses to move data within its cloud environment. The file transfer application, which is called MOVEit, is provided by Progress Software Corporation.

We now understand that one or more unauthorized individuals exploited this vulnerability in the MOVEit application and were able to access the data in certain PTA files that were queued for transfer from Envision to PTA by the MOVEit application at the time of unauthorized access. Envision has informed us that upon becoming aware of the incident ISCorp took immediate steps to secure its cloud environment, began an internal investigation, and hired a leading computer forensic firm to assist. Furthermore, Envision has stated that, according to ISCorp's forensics investigation of the incident, the unauthorized individuals had access to PTA's files containing shareholder information for approximately eight (8) minutes, and no internal systems of Envision or PTA were affected.

Envision initially notified PTA about this incident and the possibility it may have affected PTA files on June 5, 2023. PTA immediately notified its internal incident response team and engaged its third-party IT provider for support in assessing and responding to the incident. Envision thereafter provided PTA with updates on the status of its investigation, while PTA

continued to seek information from Envision regarding the nature, scope, and extent of the incident, as well as confirmation that the incident has been properly contained and fully remediated. On June 14, 2023, PTA received written notification from Envision confirming the impact of the security incident on the personal information of Pear Tree Fund shareholders. The information that was accessed without authorization included

.

Both ISCorp and Envision have assured us that they have taken additional steps to enhance their data security practices with respect to Pear Tree Funds shareholder data held within ISCorp's private cloud environment, including by following the course of action recommended by Progress Software Corporation, and by implementing additional technical safeguards. In addition, Pear Tree Advisors is implementing additional data protection measures recommended by Envision to protect shareholder personal information and has instituted new shareholder-verification procedures intended to prevent unauthorized individuals from making changes to shareholders' Pear Tree Funds accounts. PTA is also offering affected shareholders complimentary membership in ' identity theft protection services through Experian called IdentityWorks, which includes of credit monitoring, a $1,000,000 identity-theft insurance policy, and fully managed identity-theft recovery services.

Please find attached to this letter as Exhibit 1 a copy of the template notification letter that is being mailed to all affected Pear Tree Fund shareholders concurrently with our sending of this letter.

Please let me know if you have any questions regarding this matter. Thank you.

Respectfully,

Peter J. Guffin

Enclosure

EXHIBIT 1

Template Consumer Notification

Please see attached.

Return Mail Processing
PO Box 999
Suwanee, GA 30024

1 1 1 **********AUTO**MIXED AADC 300
SAMPLE A. SAMPLE -
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

July 7, 2023

Notice of Data Security Incident

Dear Sample A. Sample:

Pear Tree Advisors, Inc. ("PTA"), the transfer agent of Pear Tree Funds ("PTF"), values the privacy and confidentiality of PTF shareholders' personal information and takes the protection of that information very seriously. Regrettably, this letter is to inform you about a recent data security incident that involved some of your personal information. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened? PTA recently received notification from Envision Financial Systems, Inc. ("Envision"), the provider of PTA's investor management software, that a private cloud environment managed by Envision's subcontractor Integrated Systems Corporation ("ISCorp") experienced a data security incident that compromised certain PTF shareholder information. ISCorp utilizes a widely used file transfer software application called MOVEit, which is provided by Progress Software Corporation, to move files within the ISCorp environment. We now understand that one or more unauthorized individuals exploited a vulnerability in the MOVEit application and were able to access the data of hundreds of government agencies and businesses, including PTA's. We have been advised that upon becoming aware of the incident, ISCorp immediately took steps to secure its cloud environment, began an internal investigation, and hired a leading computer forensic firm to assist. We also have been informed that ISCorp's internal investigation showed that a limited number of PTA files containing PTF shareholder information were accessed for approximately eight (8) minutes on May 31, 2023 without authorization through the MOVEit vulnerability. At this time, neither ISCorp, Envision, nor PTA is aware of any fraudulent activity against those PTF shareholders as a result of this incident, however, we cannot rule out such activities and therefore wanted to inform you of this incident out of an abundance of caution.

Please note that, although investigation of this incident is still ongoing, based on a forensics analysis conducted by ISCorp, it is our understanding that this incident did not involve or affect any of the internal systems of Envision or PTA. Accordingly, we believe that the only information compromised by the incident was limited to PTF shareholder information queued for transmission from Envision to PTA at the time of unauthorized access.

What Information Was Involved? The compromised files included
.

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. Envision has assured us that both it and ISCorp are enhancing their data security practices with respect to data held within ISCorp's private cloud environment, including by implementing additional technical safeguards. In addition, PTA has adopted certain data protection measures recommended by Envision to further protect shareholder personal information processed using Envision's software and has instituted new shareholder-verification procedures intended to prevent unauthorized individuals from making changes to shareholders' PTF accounts.

Additionally, to help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for .

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at . Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

What You Can Do. Additional information about what you can do to protect your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information. Your trust is our top priority, and we deeply regret any inconvenience or concern caused by this incident. If you have further questions or concerns about the incident, or would like an alternative to enrolling online, please call toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please be prepared to provide your engagement number

Sincerely,

Willard L. Umphrey
President & Director
Pear Tree Advisors, Inc.

Additional Steps You Can Take to Further Protect Your Information

1. **Review your account statements and credit reports**. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission ("FTC").

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

2. Obtain and Monitor your Credit Report. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the FTC's website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

3. Consider Placing a Fraud Alert on Your Credit Report. If you choose to place a fraud alert on your credit report, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by contacting them using the information below. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Additional information is available at www.annualcreditreport.com.The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only 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 will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files. The following information must be included when requesting a security freeze (note that if you are requesting a credit freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain information from the credit reporting agencies and the FTC about security freezes.

5. Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. For more information, please visit https://consumer.ftc.gov/identity-theft-and-online-security, IdentityTheft.gov, or call 1-877-ID-THEFT (877-438-4338).

Maryland Residents: Maryland residents may review information provided by the Maryland Attorney General on how to avoid identity theft at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or by calling 410-576-6491.

Massachusetts Residents: Under Massachusetts law, Massachusetts residents have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: New York residents may contact the following state agencies that provide information regarding security breach response and identity theft prevention and protection information: the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and the New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

North Carolina Residents: North Carolina residents may obtain information about steps you can take to prevent identity theft from the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/ or at: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (toll-free within North Carolina) or 1-919-716-6400.

Rhode Island Residents: Rhode Island residents may request additional information by contacting the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903; or online at: www.riag.ri.gov; or by telephone at: 1-401-274-4400.