Steelhead Partners, LLC

[Date]

[Name]
[Address]

Re: Notice of Data Breach by IRS Contractor

What Happened?

On behalf of Steelhead Pathfinder Fund, L.P. ("Pathfinder"), we are writing to inform you that we were recently notified by the Internal Revenue Service ("IRS") of an incident concerning Pathfinder tax information. This incident involved an IRS contractor's improper treatment of IRS data associated with thousands of individuals. We received the attached notification from the IRS on April 18, 2024, stating that the Department of Justice had criminally charged the contractor with illegally inspecting or disclosing Pathfinder's federal tax returns (presumably, among many others). Per the notification letter, the tax returns were accessed by the contractor between 2018 and 2020, and, per the Factual Basis for Plea in the criminal case, the access included returns and return information dating back over 15 years.[1]

Pathfinder's federal tax returns are required to include a copy of all Form K-1s that are issued to limited partners. Form K-1 includes the limited partner's name, address and taxpayer identification number (meaning for individuals, and certain disregarded trusts, Social Security number). While the notification letter, which is the only information we have received from the IRS, specifies that the contractor has been charged with unauthorized inspection or disclosure of Pathfinder's tax returns, at this point we are unable to determine whether Pathfinder's tax returns (and limited partners' K-1s) were disclosed or merely inspected by the charged individual. Out of an abundance of caution, and in accordance with state legal requirements, we are notifying you so that you may take steps to protect yourself (while also noting that the criminal activity ceased almost four years ago).

At Steelhead Partners, we take information security very seriously. All the data provided to the IRS is (and was) legally required and properly provided as part of Pathfinder's tax returns and, to our knowledge, the unauthorized inspection or disclosure involved only the IRS database (and did not involve any of Steelhead's networks, systems, or databases). Therefore, this incident, while regrettable, was completely out of our control.

What Information was Involved?

According to the IRS letter this incident may have included the information we are required to include in our tax return: your name, address and Social Security number as shown on the Form K-1 you received from us.

What We are Doing.

We are notifying all individual (and disregarded trust) limited partners whose Form K-1 was included in our tax returns that were filed between Pathfinder's inception and 2020 to provide steps you may take to protect yourself against any potential misuse of your personal information.

[1] The Department of Justice has provided an online source for information about the criminal case. It can be accessed at https://www.justice.gov/criminal/criminal-vns/case/united-states-v-charles-littlejohn. According to this site, on January 29, 2024, the defendant was sentenced to five years in prison by the U.S. District Court for the District of Columbia.

To help protect your identity, we are offering a complimentary 24-month membership of Experian's® IdentityWorks℠. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: August 30, 2024 (your code will not work after 5:59 pm CT on this date.)
- **Visit** the Experian IdentityWorks website to enroll: http://www.experianidworks.com/credit (using a different URL may make the codes unusable or create errors during enrollment)
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332 (available Monday through Friday from 8 am – 8 pm CST (excluding major U.S. holidays)) by August 30, 2024**.** Be prepared to provide engagement number B123075 as proof of eligibility for the identity restoration services by Experian.

What You Can Do.

You should remain vigilant for incidents of fraud and identity theft including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.consumer.gov/idtheft, call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. If you believe you are a victim of identity theft, you may also notify the IRS by completing Form 14039 (Identity Theft Affidavit), available here: https://www.irs.gov/dmaf/form/14039.

You may also periodically obtain free credit reports from each nationwide credit reporting agency. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to keep an eye on the accuracy and completeness of the information in your reports. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(888) 378-4329	(888) 397-3742	(800) 680-7289
P.O. Box 740241	P.O. Box 9554	Fraud Victim Assistance Division
Atlanta, GA 30374	Allen, TX 75013	P.O. Box 2000
www.equifax.com	www.experian.com	Chester, PA 19016-2000
		www.transunion.com.

If you discover information on your credit report arising from a fraudulent transaction, then you should request that the credit reporting agency delete that information from your credit report file.

For More Information.

In addition, you may obtain further information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You may add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to

obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you may contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization.

Please know that we sincerely regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact us at 1-800-660-3556 if you have any questions or concerns.

Sincerely,

Brent E. Binge
General Counsel and Chief Compliance Officer

Enclosure

IF YOU ARE A CALIFORNIA RESIDENT: Even if you do not find any signs of fraud on your credit reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. The law allows you to order a free credit report from each agency every 12 months. You may order one, two, or all three reports at the same time, or you may stagger your requests during a 12-month period to monitor the accuracy and completeness of the information in your reports. Just call one of the numbers above to order your report and keep the "fraud alert" in place. For more information on identity theft, you may visit the California Office of Privacy Protection website, www.oag.ca.gov/privacy.

IF YOU ARE A MARYLAND RESIDENT: You may obtain information from these sources about steps to avoid identity theft from the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov, 1-888-743-0023 toll-free; from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.consumer.gov/idtheft, (877) IDTHEFT (438-4338); or from the three consumer reporting agencies whose information is listed above.

IF YOU ARE A NEW YORK RESIDENT: For more information on identity theft, we suggest that you visit the New York State Consumer Protection Board website at www.dos.ny.gov/consumerprotection.

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com