<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



<<Date>> (Format: Month Day, Year)

NOTICE OF DATA BREACH

Dear <<First_name>> <<Last_name>>,

We are writing to notify you that Point72 Asset Management, L.P. ("Point72") recently experienced a cybersecurity incident. As a global alternative investment firm, Point72 sometimes receives information (including personal information) from third parties, including in connection with investments that Point72's affiliates are considering making in various companies. This notice provides you with information about the incident and explains the steps we have taken in response, including the services we are making available to you. Please read this notice carefully.

What Happened?

Like other financial services firms, Point72 recently experienced a social engineering incident involving the compromise of two Point72 user accounts by an unauthorized third party. Based on our investigation, we determined that the first account was compromised on July 31, 2026, and the second account was compromised on August 3, 2026. The unauthorized third party was able to use the accounts to copy certain files from limited portions of our IT systems. We discovered the unauthorized access on August 1 (account one) and August 4 (account two), respectively. We promptly contained the unauthorized access, engaged leading outside data security experts to investigate, and notified law enforcement. Our experts have confirmed our containment efforts were effective, and we have seen no unauthorized access to our systems since August 4.

What Information Was Involved?

Our investigation has recently determined that some of your personal information was included in materials accessed by the unauthorized third party, including your <<b2b_text_1 (data elements)>><<b2b_text_2 (data elements cont.)>>.

We have no evidence that your information has been used for identity theft or fraud at this time.

What We Are Doing

Point72 takes this incident very seriously, and we have taken a range of steps to further enhance our existing security controls.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

If you have questions, please call (844) 971-8640, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Please have your membership number ready.

What You Can Do

We strongly encourage you to take advantage of the identity monitoring services we are providing to you free of charge. Remain vigilant and carefully review your online and financial accounts, account statements, and free credit reports for any suspicious activity. Please review the attached "Additional Important Information" document for more steps you can take.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account and promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to the proper law enforcement authority.

Should you have questions or concerns regarding this matter, please do not hesitate to contact Gina DiMento at [redacted]

Sincerely,

Point72 Asset Management, L.P.

Additional Important Information

1. Reviewing Credit Reports. We recommend that you monitor your credit reports for any activity you do not recognize. Under U.S. law, you are entitled to one free credit report every 12 months from each of the three major credit bureaus. To obtain a free annual credit report, visit www.annualcreditreport.com or call 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it 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. If you see anything in your credit report that you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

2. Place Fraud Alerts. At no charge, you can also have the credit bureaus place a "fraud alert" on your credit file. A fraud alert tells creditors to follow certain procedures to verify your identity, including contacting you, before they open any new accounts or change your existing accounts. Please note that placing a fraud alert may cause a delay when you seek to obtain credit. You can learn more about fraud alerts by contacting the credit bureaus or by visiting their websites as set forth below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/ 1-888-298-0045	https://www.experian.com/help/ 1-888-397-3742	https://www.transunion.com/credit-help 1-800-680-7289
Equifax Information Services LLC (Fraud Alert) P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Victim Assistance P.O. Box 2000 Chester, PA 19016
Equifax Information Services LLC (Credit Freeze) P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094

To place a fraud alert, contact any one of the above bureaus using 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. Placing Security Freezes. A security freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security 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.

To place a security freeze, you must contact all three of the above bureaus and may be required to provide your full name; SSN; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.

4. Monitoring Your Account Statements. We encourage you to carefully monitor your financial account statements for fraudulent activity and report anything suspicious to the respective institution or company with which the account is maintained. You should also promptly report any fraudulent activity or suspected incident of identity theft to law enforcement, your state Attorney General, and/or the FTC. The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 866-653-4261. The FTC encourages those who discover that their information has been misused to file a complaint with them.

You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information about you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.ftc.gov/credit.

5. State Specific Notices. Residents of the following states should review the following:

California and Wyoming residents: This notice was not delayed as a result of a law enforcement investigation.

Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://www.oag.dc.gov/, 1-202-727-3400. to obtain information about steps to take to avoid identity theft.

Iowa and Oregon Residents: You are advised to report any suspected identity theft to local law enforcement, the Federal Trade Commission, and your state Attorney General.

Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, 1-888-743-0023 for information on steps to take to prevent identity theft.

Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

New York Residents: You can obtain additional information about identity theft prevention and protection from the New York State Attorney General's Office, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/. The Division of Consumer Protection can be reached at: 1-800-697-1220; https://dos.ny.gov/consumer-protection.

North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226 to obtain information about preventing identity theft.

Rhode Island residents: For more information on how to prevent identity theft, you may contact the Rhode Island Attorney General at 150 South Main Street, Providence, RI 02903, (401) 274-4400, and https://riag.ri.gov/. You have the right to file a police report about this incident. Placing a security freeze on your credit file with the three credit reporting agencies does not require a fee. [redacted]

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services from Kroll for <<ServiceTerminMonths>> months:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.