Akin Gump
STRAUSS HAUER & FELD LLP

NATASHA G. KOHNE
+1 415.765.9505/fax: +1 415.765.9501
nkohne@akingump.com

August 19, 2020

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

New Hampshire Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

To the New Hampshire Office of the Attorney General:

We represent First Pacific Advisors, LP ("FPA") and write to notify you about an incident that may affect the security of some personal information relating to two New Hampshire residents, as further described below. FPA is a Los Angeles-based investment adviser registered with the Securities and Exchange Commission located at 11601 Wilshire Blvd, Los Angeles, CA 90025. We write to inform you of the nature of the incident and to explain the steps that FPA is taking to address the incident, including notifying potentially impacted individuals and identifying ways to help them protect their personal information.

Nature of the Incident

FPA recently determined that two employee email accounts were temporarily accessed by an unauthorized third party who sent a phishing email that impersonated a company service provider. Upon learning of the situation, FPA promptly contained the incident by securing the email accounts, immediately took remedial actions and launched an investigation with the assistance of an independent expert computer forensics firm.

The investigation determined that between May 2, 2020 and May 5, 2020, the two email accounts were accessed by a third party without authorization. After performing a thorough review to determine who and what information was affected and completing the investigation on or around July 21, 2020, we concluded that the incident did not extend beyond the two email accounts. As part of the investigation, it was concluded that one or more of the following types of personal information were present in the two affected email accounts at the time of the incident: name, mailing address, telephone number, email address, date of birth, social security number, and employee health insurance information.

There is no evidence that the unauthorized third party viewed the personal information. However, as a precaution, we are nonetheless notifying this Office and the individual state residents, including providing them with complimentary credit monitoring and identity theft restoration services for 24 months.

Residents Notified

FPA has identified those affected individuals who are residents in your state and the personal information of such residents that was present in the two email accounts, and FPA intends to provide notice of the incident to two New Hampshire residents on or about August 20, 2020. An unaddressed copy of the individual notification letter is attached.

Steps Taken Relating to the Incident

After learning about the incident, FPA quickly took steps to confirm the security of its systems, including all of its employee email accounts. FPA immediately reset the passwords for the affected email accounts, and required all other employees not affected by the incident to reset their passwords. FPA has been implementing additional safeguards designed to protect its network and has increased the intensity of its phishing testing, including targeted training. FPA also contacted federal and state authorities. In addition, FPA is providing a telephone number for individuals to call with any questions they may have.

By providing this notice, FPA does not waive any rights or defenses regarding the applicability of New Hampshire law, personal jurisdiction or other related rights. Please do not hesitate to contact me at (415) 765-9505 or nkohne@akingump.com if you have any questions regarding this matter.

Sincerely,

Natasha G. Kohne

Attachment

FPA
investors first
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 20, 2020

F7224-L03-0000003 T00001 **********SINGLE PIECE
SAMPLE A SAMPLE - L03 NATURAL PERSON NOTICE
APT #123
123 ANY ST
ANYTOWN, US 12345-6789

Notice of Data Breach

Dear Sample A Sample,

At First Pacific Advisors, LP ("FPA"), we take seriously our commitment to protecting your personal information. Unfortunately, we were the victim of an email phishing incident involving some of your personal information. Although at this time we have no information that would indicate that your personal information has been misused in relation to this incident, we are providing you with information about the incident, our response to it and resources available to you to help protect your personal information, should you feel it appropriate to do so.

What happened?

We recently discovered that two employee email accounts were temporarily accessed by a perpetrator who sent a phishing email that impersonated an FPA service provider. Upon learning of the situation, we promptly contained the incident by securing the email accounts, immediately took remedial actions and launched an investigation with the assistance of an independent expert computer forensics firm.

The investigation determined that between May 2, 2020 and May 5, 2020, the two email accounts were accessed by a third party without authorization. After performing a thorough review to determine who and what information was affected and completing the investigation on or around July 21, 2020, we concluded that the incident did not extend beyond the two email accounts, and that there is no evidence that the perpetrator viewed your personal information. However, we cannot rule out this possibility, as some of your personal information was contained in those email accounts.

What information was involved?

Our investigation determined that at the time of the incident your [redacted] were present in the affected email accounts.

What are we doing to protect your information?

The privacy and security of your personal information are among our highest priorities. After learning about the incident, we quickly took steps to confirm the security of our systems, including all of our employee email accounts. We immediately reset the passwords for the affected email accounts, and we required all other employees not affected by the incident to reset their passwords. We continue to implement additional safeguards designed to protect our network and your personal information, and we increased the intensity of our phishing testing, including targeted training. We also contacted federal and state authorities.

As a precautionary measure to further safeguard your personal information at your option, we have secured the services of Experian to provide complimentary credit monitoring and identity restoration services. FPA will cover the costs of these services; however, you will need to activate these services yourself.

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with superior 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: November 30, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code: ABCDEFGHI**

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 (866) 362-1769 by **November 30, 2020.** Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 24-month 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.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. 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 (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 this Identity Restoration support is available to you for two years 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. You will also find self-help tips and information about identity protection at this site.

What can you do?

Please review the enclosed "Additional Resources" document which describes additional steps you can take to help protect yourself, including recommendations by the U.S. Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We also recommend that you remain vigilant to detect suspicious activity and to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely.

For more information.

We understand you may have questions about this incident that may not be addressed in this notice. If you have additional questions please contact our FAQ call center at (866) 362-1769 between 6:00 AM to 8:00 PM (Pacific) and Saturday and Sunday 8:00 AM to 5:00 PM (Pacific).

We sincerely regret any inconvenience or concern this may have caused and continue to review and further enhance our information security practices. As a firm, we are committed to the privacy and security of your personal information.

Sincerely,

J. Richard Atwood
Managing Partner
First Pacific Advisors, LP
11601 Wilshire Boulevard, Suite 1200 | Los Angeles, CA 90025 | T310.473.0225

* Offline members will be eligible to call for additional reports quarterly after enrolling

** 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.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-298-0045
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-916-8800

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105283, Atlanta, GA 30348-5283.

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report 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.

As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.freeze.equifax.com
1-888-298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

TransUnion Consumer Solutions
P.O. Box 2000
Chester, PA 19016-2000
freeze.transunion.com
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed below.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut residents, the Attorney General may be contacted at: Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106; www.ct.gov/ag; 1-860-808-5318.

For Maryland residents, the Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD, 21202; www.marylandattorneygeneral.gov; 1-888-743-0023;
Consumer Hotline 1-410-528-8662.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. The Attorney General may be contacted at: Office of the Attorney General, One Ashburton Place, Boston, MA 02108; www.mass.gov/ago/contact-us.html; 1-617-727-2200.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/; 1-800-771-7755. The New York State Division of Consumer Protection may be contacted at: New York Department of State, Division of Consumer Protection, 99 Washington Avenue, Suite 650, Albany, NY 12231; http://www.dos.ny.gov; 1-800-697-1220.

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; www.ncdoj.gov; 1-877-566-7226 or 1-919-716-6400.

For Oregon residents, you are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General. The Attorney General may be contacted at: Oregon Department of Justice, Office of the Attorney General, 1162 Court St. NE, Salem, OR 97301-4096; www.doj.state.or.us; 1-503-378-6002; Consumer Hotline: 1-877-877-9392.

For Rhode Island residents, the Attorney General may be contacted at: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. This incident affected approximately one Rhode Island resident.

For Washington, DC residents, the Attorney General may be contacted at: Office of the Attorney General, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; https://oag.dc.gov/; 1-202-727-3400.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.