



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

August 21, 2024

L8615-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 INDIVIDUAL



APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY



Subject: Notice of Data [Extra1]

Dear Sample A. Sample:

We are writing to notify you of a cybersecurity incident at Keystone Pacific Property Management (“Keystone”) that affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On December 17, 2023, Keystone became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, Keystone immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. Based on that investigation, we learned that certain files from our network were acquired without authorization, some of which contained individuals’ personal information. We then engaged a third-party vendor to commence a comprehensive review of the impacted data to determine precisely what may have been affected and the individuals involved. That process concluded on August 19, 2024, and identified your information as potentially impacted which is the reason for this notification. Please note that Keystone has no evidence of any actual or suspected misuse of information involved in this incident.

What Information Was Involved? The information involved this incident may have included your name and your [Extra2].

What We Are Doing: As soon as we discovered this incident, we took steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our security posture and reduce the risk of similar future incidents.

We are also offering you access to complimentary credit monitoring and identity theft protection services through services through Experian IdentityWorks - a data breach and recovery services expert. These services include ## months of credit¹ and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

¹ To receive credit monitoring 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.

0000001



To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** November 29, 2024 (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 or need assistance with enrolling, please contact Experian's customer care team at 1-866-242-1607 by November 29, 2024.

You are automatically eligible for Experian identity restoration services for ## months from the date of this letter (www.ExperianIDWorks.com/restoration). Please be prepared to provide engagement number ENGAGE# as proof of eligibility.

What You Can Do: We recommend that you review the guidance included with this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you through Experian IdentityWorks by using the activation code provided above.

For More Information: Further information about how to help protect your information appears on the following page. If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call Experian at 1-866-242-1607 Monday through Friday from 6 am – 6 pm Pacific (excluding major U.S. holidays).

Sincerely,

Mike Hunsche

Mike Hunsche
Chief Information Officer
Keystone Pacific Property Management
16775 Von Karman Ave, Ste 100
Irvine, CA 92606

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

0000001



You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; [202-727-3400](tel:202-727-3400); oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Oregon: Oregon Office of the Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR, 97301, 1-877-877-9392, www.doj.state.or.us

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>. The total number of Rhode Island residents receiving notification of this incident is 0.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov

ADDITIONAL DETAILS REGARDING YOUR ##-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.
- Internet Surveillance: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- 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.

* 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.

0000001



