

We represent Pyramid Advisors Limited Partnership d/b/a Pyramid Global Hospitality (“Pyramid”) located at 30 Rowes Wharf, Suite 530, Boston, Massachusetts 02110 and write to provide notice of a data event.

On or about August 14, 2025, Pyramid became aware of suspicious activity on its network. Upon becoming aware of the event, Pyramid promptly launched an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. This investigation initially determined that while there was suspicious activity, there were no indications that data was impacted.

Subsequently on September 30, 2025, Pyramid discovered that data on its servers was impacted by this event. Pyramid then began a comprehensive review of the impacted data with the assistance of a third-party specialist, to determine what information was affected and to whom the information related. Pyramid is providing this notice after determining that current and former Pyramid employee data was likely impacted by this event. Pyramid is continuing to review the impacted data and will provide a subsequent update if the impacted population materially changes.

Pyramid’s investigation determined that the following types of information could have been present in the impacted servers at the time of the event: name, Social Security number, driver’s license number or state identification number, other governmental identification numbers, financial account information, health insurance information, and medical information. At this time, Pyramid cannot confirm that all of the foregoing information was impacted.

Pyramid provided preliminary notice of this event to its employees on October 29, 2025, and provided an offering of free credit monitoring.

On or about February 25, 2026, Pyramid continued providing written notice of this event to potentially affected individuals.

Upon becoming aware of the event, Pyramid took action to investigate and respond, evaluate the security of its systems, and notify individuals who might be affected. Pyramid is also enhancing administrative and technical safeguards and providing additional employee training. Additionally, Pyramid is offering credit monitoring and identity restoration services through IDX at no cost to those whose personal information may have been impacted.

Pyramid is providing impacted individuals with guidance on protecting against identity theft and fraud, including advising them to report incidents to their credit card company or bank. They are offering information on placing fraud alerts and credit freezes, contact details for consumer reporting agencies, instructions for obtaining free credit reports, and reminders to monitor account statements for fraud. Additionally, Pyramid encourages reporting identity theft to the FTC, state attorneys general, and law enforcement. Pyramid has notified relevant state regulators and federal law enforcement. Finally, Pyramid notified the consumer reporting agencies including Experian, Equifax, and TransUnion.

 **PYRAMID**
GLOBAL HOSPITALITY
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>

Enrollment Deadline: May 25, 2026

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

February 25, 2026

<<Variable Data – Variable letter header>>

Dear <<First Name>> <<Last Name>>:

Pyramid Advisors Limited Partnership d/b/a Pyramid Global Hospitality (“Pyramid”) recognizes the importance of protecting the information we maintain. We are writing to notify you that we identified and addressed an event that involved some of your personal information. This notice explains the event, measures we have taken, and additional steps you may consider taking in response. If you are a current Pyramid employee, you may have received notice of this same event in October 2025.

What Happened? On or about August 14, 2025, we became aware of suspicious activity on our network. Upon becoming aware of the event, we promptly launched an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. This investigation initially determined that while there was suspicious activity, there were no indications that any of our data was impacted. Subsequently on September 30, 2025, we discovered that data on our servers was impacted by this event. We then began a comprehensive review of the impacted data with the assistance of a third-party specialist, to determine what information was affected and to whom the information related. We are providing this notice after determining that current and former Pyramid employee data was likely impacted by this event.

What Information Was Involved? Our investigation determined that the following types of information related to you may have been present in the impacted servers at the time of the event: name, Social Security number, driver’s license number or state identification number, other governmental identification numbers, financial account information, health insurance information, and medical information. At this time, we cannot confirm that all of these types of information related to you were impacted.

What We Are Doing. We take this event and the security of personal information in our care very seriously. Upon learning of the activity, we took steps to ensure the security of our systems, investigate the event, and report the event to federal law enforcement. Additionally, we are notifying state regulators as required. We also recognize the evolving nature of cyber security and will continue to evaluate and enhance our safeguards. While we have no evidence of identity theft or fraud related to this event, as an added precaution, we are providing you with access to 12 months of complimentary credit and CyberScan monitoring services through IDX. Information on how to enroll in these services is on the proceeding pages. Please note, we are not permitted to enroll you in these services and so you will need to follow the instructions included below to enroll. **Please note the deadline to enroll is May 25, 2026.**

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the proceeding pages with more steps you can take.

For More Information. If you have additional questions, please contact our dedicated assistance line at [REDACTED] between 9:00 AM to 9:00 PM Eastern Time, Monday through Friday (excluding major US holidays). You may also write to us at 30 Rowes Wharf, Suite 530, Boston, MA 02110.

Sincerely,
Pyramid Global Hospitality

ADDITIONAL INFORMATION

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note, you must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers can place a free fraud alert on their credit file. An initial alert lasts one year, requiring businesses to verify identity before granting credit. Identity theft victims qualify for a seven-year extended alert. Contact the three major credit bureaus to set up a fraud alert.

Alternatively, consumers can request a free credit freeze, blocking access to their credit report without authorization. This prevents unauthorized accounts but may delay approval for future credit applications. Federal law prohibits fees for placing or lifting a freeze. To initiate, individuals may need to provide some or all the following information.

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission (FTC), or their state attorney general. The FTC may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The FTC also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers

have the right to file a police report if they ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://oag.maryland.gov>.

For Massachusetts Residents, Under Massachusetts law, consumers have the right to obtain any police report filed in connection to this event (if available). If a consumer is the victim of identity theft, they also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [REDACTED] Rhode Island residents that may be impacted by this event.