

EXHIBIT 1

By providing this notice, Bunkhouse Management, LLC (“Bunkhouse”) does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about July 17, 2024, Bunkhouse became aware of unauthorized system activity and promptly began an investigation to confirm the nature and scope of the issue. Through the investigation, it was determined that between June 4 and June 30, 2024, an unauthorized person viewed and/or copied files stored on certain Bunkhouse systems. Bunkhouse conducted a thorough review of those files to determine whose personal information was present and identify contact information for those individuals. This review was recently completed and Bunkhouse is now providing notice to relevant individuals. The information related to Nebraska residents that was present in the reviewed files included name, Social Security number or individual taxpayer identification number, and driver’s license or state license number.

Notice to Nebraska Residents

On or about April 15, 2025, Bunkhouse provided written notice of this event to two (2) Nebraska residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

In response to this event, Bunkhouse moved quickly to assess the security of systems, conduct a diligent investigation into the nature and scope of this event, review the content of the relevant data for sensitive information and to whom the information belonged, and identify contact information for individuals. Further, Bunkhouse notified federal law enforcement regarding the event. Bunkhouse is also working to implement additional safeguards and training to its employees.

Bunkhouse is providing access to credit monitoring services for twelve (12) months, through Cyberscout, a TransUnion Company, to individuals whose information was potentially affected by this event, at no cost to these individuals. Additionally, Bunkhouse is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Bunkhouse is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Bunkhouse is providing written notice of this event to relevant state regulators, as necessary.

EXHIBIT A



0001623

Bunkhouse Management, LLC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS366

10_0001623



Dear _____ :

Bunkhouse Management, LLC ("Bunkhouse") is writing to make you aware of a incident that may involve your personal information. Although Bunkhouse is unaware at this time of any identity theft or fraud in relation to this event, this letter provides you with details about the event, our response, and steps you can take to better protect yourself, should you feel it appropriate to do so.

What Happened? Bunkhouse learned of unauthorized system activity and promptly began an investigation. The investigation determined that, in or around June 2024, an unauthorized person viewed and/or copied certain files stored on certain Bunkhouse systems. Bunkhouse conducted a thorough review of those files to determine whose personal information was present and identify contact information for those individuals. You are now receiving this letter because we found your information in the relevant files.

What Information Was Involved? We determined that your name, and Social Security number or individual taxpayer identification number, driver or state license number, health insurance information, medical information, financial account information, and payment card information were present in the relevant files.

What We Are Doing. We take the privacy of information in our care very seriously. In response to this event, we promptly took steps to secure our systems and conduct a diligent investigation. We recognize the evolving nature of cyber security and will continue to take steps to review and enhance our safeguards in the future. We are also providing you with guidance on ***Steps You Can Take to Help Protect Your Personal Information***, which can be found in the attachment to this letter. As an added precaution, we are offering you access to twelve (12) months of credit monitoring and identity theft protection at no cost to you. Information on these services and directions on how to enroll are included in ***Steps You Can Take to Help Protect Your Personal Information*** attachment to this letter.

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 information contained in the attached ***Steps You Can Take to Help Protect Your Personal Information*** and enroll in the credit monitoring services we are offering. Please note, we are not able to enroll you, so you will need to follow the instructions below to take advantage of these services.

For More Information. If you have additional questions or need assistance, please contact our dedicated assistance line at 1-833-998-8083 Monday through Friday, between the hours of 8 a.m. and 8 p.m. Eastern Time. You may also write to us at 1711 South Congress Avenue, Suite 300, Austin, Texas 78704.

Sincerely,

Bunkhouse Management, LLC
<https://www.bunkhousehotels.com/>

Steps You Can Take To Help Protect Your Personal Information

Enroll in Monitoring Services

In response to the matter, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted, please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your 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 <https://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 have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 credit freeze or fraud alert, 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/data-breach-help/
1 (888) 298-0045	1 (888) 397-3742	1 (833) 799-5355
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

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; <https://www.identitytheft.gov>; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission 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 in order 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 <https://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://www.marylandattorneygeneral.gov/>.

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 https://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.



0001623

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 <https://www.ncdoj.gov>.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; <https://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 2 Rhode Island residents that may be impacted by this event.