

EXHIBIT 1

By providing this notice, Heartland Recreational Vehicles (“Heartland”) located at 2831 Dexter Drive, Elkhart, Indiana 46514, 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 January 26, 2025, Heartland identified indications of malicious encryption on company computer systems due to a sophisticated cyber-attack by an unknown actor. Heartland promptly undertook a comprehensive incident response with the assistance of third-party cybersecurity and digital forensics specialists. Through this investigation, Heartland determined that the unknown actor gained access to certain systems between January 26 and 27, 2025, files on a limited subset of those systems were potentially viewed and downloaded. Heartland then conducted a comprehensive third-party review of the potentially impacted files to determine what information was contained therein and to whom the information related. Heartland subsequently undertook an internal review of its records to identify contact information for potentially affected individuals to issue notifications. Heartland recently completed its review.

The personal information that could have been subject to unauthorized access for Nebraska residents includes: name and Social Security number.

Notice to Nebraska Residents

On or about May 1, 2025, Heartland began providing written notice of this event to potentially affected individuals, including approximately two (2) Nebraska residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon identifying the event, Heartland moved quickly to investigate and respond, assess the security of its systems, and identify potentially affected individuals. Heartland also reported the event to federal law enforcement. Heartland is also working to implement additional cybersecurity safeguards and training to its employees. As an additional precaution, Heartland is providing access to credit monitoring and identity restoration services for twelve (12) months, through Cyberscout, a TransUnion company, to individuals whose personal information was potentially affected by this event, at no cost to these individuals. Heartland also established a toll-free call center to address any questions or concerns from notified individuals.

Additionally, Heartland is providing potentially affected 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. Heartland 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.

Heartland is providing written notice of this event to appropriate state regulators, and to the three major consumer reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Heartland Recreational Vehicles
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



P
[Redacted]



May 1, 2025

Dear [Redacted]:

Heartland Recreational Vehicles (“Heartland”) writes to notify you of an event which may involve certain information related to you. Although there is no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to protect your information, should you feel it appropriate to do so.

What Happened? On January 26, 2025, Heartland identified suspicious activity on certain company computer systems. We immediately launched an extensive investigation to determine the nature and scope of the event, with the assistance of industry-leading cybersecurity specialists. We also promptly reported this event to federal law enforcement. Through our investigation, we determined that an unknown actor gained access to certain systems between January 26, and 27, 2025, and a subset of files on those systems was potentially viewed and downloaded.

We then conducted a comprehensive, third-party review of the potentially impacted files to determine what information was affected and to whom the information related. Following the third-party audit, we reviewed our records to determine the identities and contact information for potentially affected individuals to issue notifications. We recently completed our review.

What Information Was Involved? Our investigation determined that at the time of the event, your name and Social Security number were stored within the impacted files.

What We Are Doing. We take this event and information security seriously. Upon learning of the activity, we immediately took steps to further secure our systems and investigate the event. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to further enhance our information security posture.

As an additional precaution, Heartland is offering you access to twelve (12) months of complimentary credit monitoring and identity restoration services from Cyberscout, a TransUnion company. Details of this offer and instructions on how to activate these services are enclosed with 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. Please review the enclosed document, *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard against possible misuse of your information. You may also enroll in the complimentary credit monitoring services we are offering to you.

000010102G0500

P

For More Information. If you have additional questions, please contact our toll-free assistance line at 1-833-998-9362, Monday through Friday between the hours of 8 a.m. and 8 p.m. Eastern Time.

Sincerely,

Heartland Recreational Vehicles

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring 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 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 one-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, 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, 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; 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 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 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 [1] Rhode Island residents that may be impacted by this event.