CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Three Valley Square, Suite 305
512 E. Township Line Rd
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

JORDAN MORGAN
JMorgan@c-wlaw.com

LEI WANG
LWang@c-wlaw.com

May 8, 2026

Via Email
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

RE: Security Incident Notification

To Whom It May Concern:

We serve as counsel for Heritage Holdings LP ("Heritage"),[1] located at 16934 Frances St., Suite 200, Omaha, Nebraska 68130, and provide this notification to you of a recent data security incident suffered by Heritage. By providing this notice, Heritage does not waive any rights or defenses under Iowa law, including the data breach notification statute.

On or around September 16, 2025, Heritage became aware of certain unauthorized activity within its computer systems. Upon discovery, Heritage secured its systems and immediately engaged a third-party forensic firm to investigate the incident. Thereafter, Heritage continuously worked to identify and collect the impacted data and conducted a thorough review to determine the types of information that may have been impacted, the individuals to whom it relates, and up-to-date address information. On April 14, 2026, this process was completed.

As a Business Associate under HIPAA, we understand that Iowa's data breach statute does not apply to Heritage in connection with the subject incident.[2] Heritage is nevertheless notifying the Iowa Attorney General as

[1] Heritage is a Business Associate under the Health Insurance Portability and Accountability Act ("HIPAA"). *See* 45 CFR 160.103.

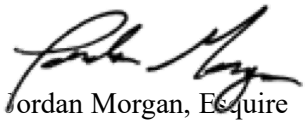
[2] "This section does not apply to…[an entity] who is subject to and complies with regulations promulgated pursuant to Tit. II, subtit. F of the federal Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §1320d – 1320d-9, and Tit. XIII, subtit. D of the federal Health Information Technology for Economic and Clinical Health Act of 2009, 42 U.S.C. §17921 – 17954." *See* Iowa Code §715C.2.7.*d.*

a professional courtesy due to the number of Iowa residents may have been affected by this incident. The potentially impacted information for Iowa residents may include first and last name, in combination with one or more of the following: Social Security number, driver's license number, account number, routing number, and protected health information.

Heritage sent written notice of this incident to approximately 2,017 potentially impacted Iowa residents on February 27, 2026, and May 8, 2026. The notification letter includes details of the incident and an offer of complimentary credit monitoring and identity protection services for 12 months and access to a dedicated call center. A copy of the notice letter is attached hereto as **Exhibit A**. Heritage continues to take proactive steps to ensure that all state and federal notification obligations are complied with due to this incident.

If you have any questions, please contact me.

Very truly yours,



Jordan Morgan, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A

Heritage Holdings LP
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

[redacted]

May 8, 2026

RE: Important Security Notification. Please read this entire letter.

Dear [redacted]:

Heritage Holdings LP ("Heritage") writes to notify you of an incident that may have impacted some of your personal information described below. Out of an abundance of caution, we are providing you information about this incident, our response, and steps you can take to help protect your information, should you feel it is appropriate to do so.

What Happened:

On or around September 16, 2025, Heritage experienced a network intrusion that affected a limited number of systems. Upon discovery, Heritage immediately took steps to secure its network and engaged a third-party forensic firm to investigate the incident. On February 9, 2026, following a full and thorough investigation, Heritage determined that a limited amount of personal information kept in the normal course of business may have been accessed by an unauthorized third party in connection with this incident. Thereafter, Heritage continued to investigate this incident to determine if any additional individuals were potentially affected. On April 14, 2026, our investigation identified that your information was located in the potentially impacted systems.

At this time, there is no indication that your information has been misused. However, we are providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that your information has been misused. The information that could have been impacted by the unauthorized individual(s) may have included your first name or initial and last name, in combination with your [redacted].

What We Are Doing:

Heritage has taken steps to address the incident and is committed to protecting personal information in its care. Upon learning of this incident, we immediately took steps to secure our network and undertook a thorough investigation. As an additional safeguard, we have arranged for you to enroll, at no cost to you, in online Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services for 12 months provided by Cyberscout, a TransUnion company. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary credit monitoring service is enclosed.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password, take additional steps to protect your account, and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center at [redacted]. Please direct any questions or concerns to this phone number, as it is the best source for the most accurate and up-to-date information. Representatives are available from 8:00 am to 8:00 pm Eastern Time, Monday through Friday, excluding major U.S. holidays. You can also write us at 16934 Frances St., Suite 200, Omaha, Nebraska 68130.

Heritage takes the security of information entrusted to our care very seriously. While it is regrettable this potential exposure occurred, please be assured that we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

Heritage Holdings LP

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Complimentary Credit Monitoring

In response to the incident, 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 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 event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. 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

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

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

concerning identity theft, if you are a victim of identity theft.

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

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California may be contacted at 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and and https://oag.maryland.gov/.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on

information in your credit report; and you may seek damages from violator. You 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 you to review your 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, you have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.