artemishealthcare inc

P.O. Box 989728
West Sacramento, CA 95798-9728

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

December 23, 2025

<<Variable Text 2: Subject Line>>

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

Artemis Healthcare, Inc. ("Artemis") writes to inform you of a recent data incident that may involve your information. Artemis provides <<Variable Text 3: Artemis's Description>>, and we have your information in relation to these services. This letter provides information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate.

What Happened? On May 31, 2025, Artemis learned of suspicious network activity, the result of our organization being the target of a cybersecurity attack by a ransomware group. Upon becoming aware of this event, Artemis promptly took steps to ensure the security of our systems, including force changing passwords and terminating active sessions. Artemis immediately launched an investigation and worked with the assistance of third-party forensic specialists to secure the network and to determine the nature and scope of the activity. Through the investigation, it was determined that there was unauthorized access to Artemis's network between May 5, 2025, and May 31, 2025. As part of the investigation, Artemis undertook a thorough review of the potentially impacted files to determine whether any sensitive information was present.

We recently concluded our investigation on September 12, 2025, and we are providing notification to potentially affected individuals.

What Information Was Involved? Based on the investigation, the potentially impacted data varies from individual to individual, and may include your name, <<Variable Text 1: Data Elements>>.

What We Are Doing. The security of information in our care is among our highest priorities, and we take this incident very seriously. In furtherance of our ongoing commitment to information security, we are reviewing our existing policies and procedures and providing additional training for our employees. We are also providing notice of this incident to potentially impacted individuals and providing you with guidance on how to better protect your information. We have also notified relevant state and federal regulators as applicable.

What You Can Do. As a general best practice, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and free credit reports for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to your bank, credit card company, or other applicable institution. Additional information and resources are included in the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact our toll-free assistance line at 1-844-990-2040, available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time (excluding U.S. holidays). You may also write to Artemis at 658 Grassmere Park, Suite 102, Nashville, TN 37211.

Sincerely,

Artemis Healthcare, Inc.

Steps You Can Take To help Protect Personal Information

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. Consumers should be aware, however, 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/credit-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; 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. 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://oag.maryland.gov. Artemis can be contacted at 313 N. Plankinton Ave Milwaukee, WI 53203 and 1-844-990-2040.

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. Fees may be required to be paid to the consumer reporting agencies. There are approximately 8 Rhode Island residents that may be impacted by this event.