

EXHIBIT 1

By providing this notice, Wood River Health (“WRH”) does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

WRH experienced a data security incident that impacted an employee email account. WRH launched an investigation with outside assistance to confirm the nature and scope of the incident and ensure security of the email tenant. Through the investigation, WRH learned that an unauthorized actor accessed the email account and may have viewed or acquired certain information between August 8, 2024, and September 6, 2024. WRH then undertook a comprehensive review of the involved information to determine what was contained therein and to whom it related. The review was completed on or about May 29, 2025.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to Maine Residents

On or about July 28, 2025 WRH provided written notice of this incident to sixty-four (64) Maine 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

Upon discovering the event, WRH moved quickly to investigate and respond to the incident, assess the security of WRH systems, and identify potentially affected individuals. Further, WRH notified federal law enforcement regarding the event. WRH is also working to implement additional safeguards and training to its employees. WRH is providing access to credit monitoring services for twelve (12) months, through Cyberscout through Identity Force, a TransUnion company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, WRH is providing impacted individuals with guidance on how to better protect against identity theft and fraud. WRH 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.

WRH is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Wood River Health
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



WOOD RIVER HEALTH
Caring for the Community of Dearborn



July 28, 2025

Dear [REDACTED]

Wood River Health (“WRH”) writes to make you aware of an incident that may impact the privacy of some of your information. We are providing you with notice of the incident, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? Wood River Health experienced a data security incident that impacted an employee email account. We launched an investigation with outside assistance to confirm the nature and scope of the incident and ensure security of the email tenant. Through the investigation, we learned that an unauthorized actor accessed the email account and may have viewed or acquired certain information between August 8, 2024, and September 6, 2024. We then undertook a comprehensive review of the involved information to determine what was contained therein and to whom it related. Our review was completed on or about May 29, 2025.

What Information Was Involved? Our investigation determined that your name and patient account number, account number, employer assigned identification number, medical record number, diagnosis, health insurance group number, health insurance subscriber number, treatment information, electronic/digital signature, username & password/pin/or account login, encounter number, other health insurance information, medical billing/claims information, date of birth, Social Security number, prescription/medication information, account number with routing number, treating/referring physician, and medicare/medicaid identification were contained within the impacted account. To date, there is no indication of identity theft or fraud in relation to this event.

What We Are Doing. We treat our responsibility to safeguard the information entrusted to us as an utmost priority. As such, we responded immediately to this incident and have been working diligently to provide you with an accurate and complete notice of the incident. Our immediate response to this event also included prompt and continued correspondence with federal law enforcement authorities. As part of our ongoing commitment to the privacy and security of information in our care, we have reviewed our existing policies and procedures relating to data protection and security and implemented enhanced security controls.

As an added precaution, we are providing you with [REDACTED] months of complimentary access to credit monitoring and identity restoration services through Cyberscout, a TransUnion company, as well as guidance on how to better protect your information. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter.

What You Can Do. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Information*. There, you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll.

000010102G0500

P

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call our dedicated assistance line at 1-833-397-4705, Monday through Friday from 8 am to 8 pm Eastern Time, excluding U.S. holidays. You can also write to Wood River Health at 823 Main Street, Hope Valley, RI 02832.


Sincerely,

Wood River Health

STEPS YOU CAN TAKE TO 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 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, 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 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://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 [#] Rhode Island residents that may be impacted by this event.