EXHIBIT 1

By providing this notice, Brownmed 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 February 3, 2026, Brownmed learned of suspicious activity on certain systems in its environment. Brownmed promptly launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. The investigation revealed that there was unauthorized access to certain files between January 16, 2026 and February 3, 2026. Therefore, Brownmed undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected, to whom it related, and identify address information to provide notifications. Brownmed completed this review on March 20, 2026.

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

Notice to Nebraska Resident

On April 9, 2026, Brownmed provided written notice of this incident to one (1) Nebraska resident. 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, Brownmed moved quickly to investigate and respond to the incident, assess the security of Brownmed systems, and identify potentially affected individuals. Further, Brownmed notified federal law enforcement regarding the event. Brownmed is also working to implement additional safeguards and training to its employees. Brownmed is providing access to credit monitoring services for two years, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Brownmed 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. Brownmed 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.

Brownmed is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A

Brownmed, Inc.
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

April 9, 2026

NOTICE OF DATA BREACH

Dear :

Brownmed, Inc. ("Brownmed") writes to inform you of an event that may impact the privacy of certain information related to you. Brownmed is providing this notice to ensure you are aware of the incident and to inform you of steps it is taking in response.

What Happened? On February 3, 2026, Brownmed learned of suspicious activity on certain systems in its environment. Upon learning this, Brownmed promptly launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. As a result of the investigation, Brownmed and the forensic specialists determined that certain files were accessed or taken without authorization between January 16, 2026 and February 3, 2026. Therefore, Brownmed undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected, to whom it related, and identify address information to provide notifications. Brownmed completed this review on March 20, 2026.

What Information Was Involved? The information that could have been impacted includes your name and the following types of information: financial account information.

What We Are Doing. Brownmed takes the confidentiality, privacy, and security of information in its care very seriously. Upon discovering the incident, it took immediate steps to secure the network and strengthen its security posture moving forward. Brownmed is also offering access to complimentary credit monitoring and identity restoration services through TransUnion for twenty-four (24) months. The deadline for you to enroll in these services is July 8, 2026. Please note that you will need to enroll yourself in these services, as Brownmed is not able to do so on your behalf. You can find instructions regarding how to enroll in these services in the enclosed *Steps You Can Take to Protect Personal Information*.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Personal Information* which contains guidance regarding what you can do to better protect against possible misuse of your information. You are encouraged 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 over the next twenty-four (24) months. Please report any suspected incidents of identity theft or fraud to your credit card company or bank.

For More Information. You may have questions about the incident that are not addressed in this letter. If you have questions, please call 1-800-405-6108, Monday through Friday, from 8:00 a.m. to 8:00 p.m. Eastern time, excluding holidays.

Sincerely,

Brownmed, Inc.

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

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 twenty-four (24) 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, 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 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 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 2 Rhode Island residents that may be impacted by this event.