EXHIBIT 1

By providing this notice, Pivot Health 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 or around March 13, 2026, Pivot Health became aware of suspicious activity within its Amazon Web Services ("AWS") environment. Pivot Health immediately took steps to secure its systems and launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor accessed the AWS environment at various periods of time between February 26, 2026 and March 13, 2026, and that during that period of unauthorized access, certain information contained within AWS was viewed or copied by the unknown actor. Pivot Health therefore undertook a comprehensive review of the data at risk to determine what information was potentially affected, and to whom that information related. That review recently completed.

Given the nature of Pivot Health's business, much of the data impacted in the event was not Pivot Health's data, but was data belonging to Pivot Health's clients. Therefore, additional steps were taken to determine which client of Pivot Health the impacted Nebraska residents were associated with so Pivot Health could effectuate appropriate notification to its business clients first to make them aware of the event and the impact to individuals associated with their organizations. The review and those efforts recently completed, and Pivot Health is now proceeding with notification to impacted individuals.

The information that could have been subject to unauthorized access includes name, financial account information and health insurance information.

Notice to Nebraska Residents

On or about May 13, 2026, Pivot Health provided written notice of this incident to approximately twenty-seven (27) Nebraska 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 becoming aware of the event, Pivot Health moved quickly to investigate and respond to the same, assess the security of Pivot Health systems, and identify potentially affected individuals. Pivot Health is also working to implement additional safeguards to protect against future incidents.

Pivot Health is also providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose financial information was potentially affected by this incident, at no cost to these individuals. Additionally, Pivot Health 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. Pivot Health 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.

Pivot Health is providing written notice of this incident to relevant state and federal regulators, as required, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Pivot Health is also notifying the U.S. Department of Health and Human Services and prominent media where required pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

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

[redacted]

May 13, 2026

NOTICE OF SECURITY EVENT

Dear [redacted]:

Pivot Health writes to inform you of a recent event that may affect the confidentiality of some of your information. Pivot Health is an insurance marketing company and healthcare services provider that assists its clients with obtaining health insurance coverage. Our clients include [redacted], and through our work with [redacted], we were in possession of certain [redacted] data that was impacted in this event. Although we are unaware of any identity theft or fraud occurring as a result of this event, we are providing you with information about the event, our response, and resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? On or around March 13, 2026, Pivot Health became aware of suspicious activity within our Amazon Web Services ("AWS") environment. We immediately took steps to secure our systems and launched an investigation into the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that an unauthorized actor accessed our AWS environment at various periods of time between February 26, 2026 and March 13, 2026, and that during that period of unauthorized access, certain information contained within AWS was viewed or copied by the unknown actor. Pivot Health therefore undertook a comprehensive review of the data at risk to determine what information was potentially affected, and to whom that information related. Those efforts recently completed, and Pivot Health is notifying you because the investigation determined that certain information relating to you was contained within the impacted files.

What Information Was Involved? The following types of information related to you were found in the impacted files: your name and health insurance billing and payment information, identification numbers such as member identification, person identification, certificate identification and coverage identification, and dates of coverage, date of birth, and financial account information. Pivot Health is not aware of your information being used to commit identity theft or fraud.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon becoming aware of the suspicious activity, we promptly commenced an investigation to confirm the nature and scope of the event. We are also reviewing existing security policies and have implemented additional cybersecurity measures to further protect against similar events moving forward. We are also notifying potentially impacted individuals, including you, so you may take steps to best protect your information, should you feel it is appropriate to do so.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for twelve (12) months at no cost to you, through Cyberscout, a TransUnion company. You can find information on how to enroll in these services in the enclosed *Steps You Can Take to Protect Personal Information*. We encourage you to enroll in these services as we are not able to do so on your behalf.

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. You may also enroll in the complimentary credit monitoring services we are offering. Please also review the information contained in the enclosed *Steps You Can Take to 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 **844-593-8519** Monday to Friday, from 8:00 am to 8:00 pm EST, excluding U.S. holidays. You may also write to us at 401 North Miami Avenue, Suite 205, Miami, Florida, 33127. We take this event very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Pivot 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: [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

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 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 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.