

Access2Day Health Notice of Data Event

Access2Day Health ("A2D") is providing notice of an event which may affect the privacy of information.

What Happened: On January 31, 2025, A2D identified suspicious activity related to certain employee email accounts. Upon learning of the activity, A2D immediately took steps to secure the email environment and launched an investigation into the nature and scope of the activity. The investigation determined that an unauthorized actor gained access to the email account briefly on January 31, 2025 and that certain emails and/or attachments within the email account were accessed by the unauthorized actor. As part of the investigation, A2D conducted a review of the involved emails to determine what information was within them and to whom it relates.

What Information Was Involved: The review recently concluded and on March 31, 2025 A2D notified relevant covered entities because A2D determined that information related to individuals was contained in the emails involved at the time of the incident. The potentially involved information related to individuals includes names, addresses, Social Security number, dates of birth, treatment/diagnosis information, procedure information, visit information, and member ID numbers. Please note, there is no evidence of any actual or attempted fraud or identity theft of your information as a result of this event.

What We Are Doing: The confidentiality, privacy, and security information in our care are among our highest priorities. To reduce the risk of this issue from occurring again, A2D has taken several actions to further secure its environment, including reviewing relevant processes and procedures and providing additional training to employees. A2D is also offering access to complimentary credit monitoring for individuals that may be impacted.

For More Information: If you have further questions, or believe you may be impacted by this event, please contact 1-833-918-6121, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information. You may also write to us at 1325 Barksdale Blvd., Suite 300, Bossier City, LA 71111.

What You Can Do: A2D encourages everyone to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors. If you detect any suspicious activity on your account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-916-8800

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed above.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General.