

DIVERSIFIED SERVICES ENTERPRISES NOTICE OF DATA PRIVACY EVENT

June 13, 2025 (Updated on September 10, 2026)

NOTIFICATION

Diversified Services Enterprises ("DSE") is providing notice of an event that impacted the privacy of certain individuals' information. ^

DSE is a provider of support management services to health care organizations. We are providing you with details about the event, our response, and additional measures you can take to help protect your information, should you feel it appropriate to do so.

What Happened? On April 14, 2025, DSE became aware of suspicious activity in our network. In response, we promptly took steps to secure our environment and launched an investigation to determine the nature and scope of the activity with the assistance of third-party forensic specialists. The investigation determined that between March 14, 2025 and April 14, 2025, certain files within DSE's network were accessed and copied without authorization. As a result, DSE engaged a data review vendor to conduct a comprehensive and time-intensive review of the contents of the affected files to identify what protected health information is contained therein and to whom that information relates. Upon receiving the results of this extensive review process from the data review vendor, DSE engaged in additional work to review and verify the affected information as well as locate address information for the potentially impacted population. DSE then worked diligently to notify potentially impacted individuals as expeditiously as possible.

What Information Was Involved? Our review determined that the following types of information were present in the affected files at the time of the event: date of birth, driver's license number or state identification card number, Social Security number, passport number, taxpayer identification number, financial account information, payment card information, medical record number, Medicare/Medicaid ID, health insurance information, and medical history information which may include: mental or physical condition, treatment information, diagnosis information and provider information. The specific type of information at issue varies per individual.

How Will Individuals Know If They Are Affected By This Incident? DSE is mailing a notice letter to individuals whose information was determined to be contained within the affected files and for whom we have a valid mailing address. If an individual does not receive a letter but would like to know if they are affected, they may call our dedicated assistance line detailed below.

What DSE Is Doing. The confidentiality, privacy, and security of personal information within our care are among DSE's highest priorities. Upon learning of the event, we promptly commenced an investigation and response that included confirming the security of our network, investigating to determine the information that was impacted, and reviewing the contents of relevant data for sensitive information. As part of our ongoing commitment to the privacy of information in our care, we are implementing additional security measures to further protect against similar incidents occurring in the future. We also reported this event to federal law enforcement and applicable government regulators, including the U.S. Department of Health and Human Services.

What You Can Do. In general, individuals should remain vigilant against incidents of identity theft and fraud by reviewing account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, healthcare provider, and/or financial institution. Additional information and resources may be found below in the Steps You Can Take to Help Protect Personal Information section of this notice.

For More Information. If you have additional questions, please call our dedicated assistance line at (844) 301-0075 between the hours of 9:00a.m. - 6:30p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a security freeze, you may need to provide 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 you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:



Equifax
<https://www.equifax.com/personal/credit-report-services/>
1-888-298-0045
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788

Experian
<https://www.experian.com/help/>
1-888-397-3742
Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013
Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013

TransUnion
<https://www.transunion.com/credit-help>
1-833-799-5355
TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
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. 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.

Copyright © 2025 DSE Incorporated - All Rights Reserved.

Powered by
 GoDaddy Airo