

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

DANIEL J. HAIER
dhaier@c-wlaw.com

KATIE GORA
kgora@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

September 6, 2024

Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Security Breach Notification

To Whom It May Concern:

We serve as counsel for Delta Health System (“DHS”), located at 1400 E Union St., Greenville MS 38703. We write to provide notification of a recent data security incident. By providing this notice, DHS does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On January 21, 2024, DHS experienced a network disruption and immediately began an investigation with the assistance of third-party specialists. The investigation determined that an unauthorized party accessed certain files on DHS’s network between approximately January 15 and January 21, 2024.

Therefore, DHS worked with a third-party data analysis firm to conduct a thorough review of the files at issue to determine the type of information contained therein and to whom the information related. This review was completed on July 8, 2024. DHS determined the files at issue included the names of 23 Maryland residents in combination with one or more of the following: Social Security number, health information, and/or health insurance information.

DHS began notifying potentially impacted individuals of this incident on March 27, 2024 and continued mailing notice letters through September 5, 2024. A copy of the notice is attached as ***Exhibit A***. DHS previously began providing notice of this incident on its website starting on March 20, 2024 while the data review was underway.

DHS has no evidence of any actual or attempted misuse of any information because of this incident. However, in an abundance of caution, DHS is offering the potentially impacted residents of Maryland complimentary access to 12 months of credit monitoring and identity protection services.

In response to this incident, DHS notified law enforcement and implemented additional network security. DHS also continues to review its policies and procedures related to data protection.

Thank you for your attention to this matter and please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

A handwritten signature in black ink, appearing to read 'D Haier', is positioned above the printed name.

Daniel Haier, Esq.
610-215-2288
dhaier@c-wlaw.com

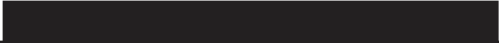


Parent/Guardian of:
<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:




Or Visit:


September 5, 2024

<<Variable Text 1: Notice of Data Breach>>

Dear Parent/Guardian of <<First Name>> <<Last Name>>:

Delta Health System writes to notify you of an incident that may affect the privacy of certain information provided to us. We take this incident seriously and are providing you the following information about the incident, our response, and steps you can take to help protect your information. Please note that we have no reason to believe any information has been or will be misused because of this incident.

What Happened? On January 21, 2024, we observed unusual activity on our computer network and immediately began an investigation with the assistance of third-party specialists. The investigation determined that certain files on our network were potentially accessed without authorization between January 15, 2024 and January 21, 2024. Therefore, we began a comprehensive review of the files at issue with the assistance of third-party specialists to determine the information they contained and to whom the information related.

What Information Was Involved? The third-party data review recently concluded and determined the potentially impacted information included your name in combination with the following: <<Variable Text 2: Data Elements>>.

What We Are Doing. In response to this incident, we worked with specialists to conduct a thorough investigation and implement additional security precautions. We also notified law enforcement and we are reviewing our policies and procedures related to data protection. While we have no reason to believe any information has been or will be misused because of this incident, we are offering you access to << Credit Monitoring Length (12/24)>> of complimentary credit monitoring and identity protection services in an abundance of caution. These services will be provided through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. The deadline to enroll is December 5, 2024.

What You Can Do. We encourage you to enroll in the complimentary credit monitoring and identity protection services we are making available to you. Information about how to enroll in these services along with additional resources available to you are included in the attached *Steps You Can Take to Help Protect Your Information*.

For More Information. We understand you may have questions about this incident. You may contact our dedicated assistance line at [REDACTED], between the hours of 8:00 a.m. to 8:00 p.m. Central time, Monday through Friday, excluding holidays, or write to us at 1400 E. Union St., Greenville, MS 38703.

We regret any concern this incident may cause you.

Sincerely,

Delta Health System

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring and Identity Protection Services

1. Website and Enrollment. Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. Telephone. Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); 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:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. 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; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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 contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.