

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Jason Goodwin
Jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

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

April 16, 2024

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: Data Breach Notification

To Whom It May Concern:

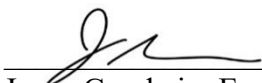
We serve as counsel for Cherry Street Services, Inc. d.b.a. Cherry Health ("Cherry Health") located at 100 Cherry Street, SE, Grands Rapids, MI 49501. We write to provide notification of a recent data security incident. By providing this notice, Cherry Health does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On December 21, 2023, Cherry Health experienced a network disruption that affected their ability to access certain systems. Upon discovery, Cherry Health took immediate steps to respond and secure the network and systems, including the engagement of third-party forensic specialists to assist in a thorough investigation into the nature and scope of the incident. Through the investigation, Cherry Health learned that certain information was accessed improperly. Cherry Health immediately worked to review its systems to determine the types of information at risk and confirm up-to-date contact information to provide individuals with notice.

On March 25, 2024, Cherry Health identified those individuals whose information may have been at risk as a result of the incident and worked to confirm up-to-date address information to provide notice, including the use of a National Change of Address (NCOA) search. On April 10, 2024, Cherry Health received its results from the NCOA search and determined this incident potentially affected 16 Maryland residents. The information potentially impacted included first and last name, addresses, phone numbers, dates of birth, health insurance information, health insurance ID number, patient ID number, provider name, service date, diagnosis/treatment information, prescription information, financial account information and/or Social Security numbers.

In response to this incident, Cherry Health took steps to secure their environment, conducted an investigation, and notified law enforcement. Additionally, Cherry Health began providing notice to the potentially impacted individuals on April 16, 2024 via U.S. mail. A copy of the notice is attached as **Exhibit A**. In an abundance of caution, Cherry Health is offering the potentially impacted individuals complimentary credit monitoring and identity protection services. Additionally, while Cherry Health's investigation into the potential impact to data remained ongoing, Cherry Health provided substitute notice of the incident pursuant to the Health Insurance Portability and Accountability Act on its website on January 24, 2024, with a subsequent update on February 15, 2024.

Very truly yours,



Jason Goodwin, Esq.

Exhibit A



Return Processing Center
PO Box 480149
Niles, IL 60714

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

Enrollment Code: <<XXXXXXXX>>
To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/CherryHealth>

April 16, 2024

<<Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>,

Cherry Street Services, Inc. ("Cherry Health") writes to notify you about a recent data security incident we experienced that may have involved your data. We take the privacy of information in our care very seriously. At this time, there is no evidence that any of your information has been, or will be, misused. In an abundance of caution, we are providing you information about the incident, our response, and steps you can take to further protect your information should you feel it is necessary to do so.

What Happened: On December 21, 2023, Cherry Health experienced a network disruption, that affected our ability to access certain systems. Upon learning of this, we immediately began an investigation with the support of third-party specialists. Through the investigation, we learned that some data we maintain was accessed improperly. We then took steps to determine the types of information that were at risk and the individuals to whom it pertained. On March 25, 2024, this process was completed, and we worked to notify you as soon as possible.

What Information Was Involved: The types of information potentially at risk may have included your first and last name, in combination with one or more of the following data elements: addresses, phone numbers, dates of birth, health insurance information, health insurance ID number, patient ID number, provider name, service date, diagnosis/treatment information, prescription information, financial account information and/or Social Security numbers.

What We Are Doing: We have implemented additional technical safeguards to further enhance the security of data we maintain and to prevent something similar from happening in the future. As an added precaution, we are making credit monitoring and identity protection services available to you for <12/24> months at no cost to you.

What You Can Do: We recommend that you remain watchful for potential incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for errors or suspicious activity. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft should you feel it appropriate to do so.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line at 888-964-4694 Monday through Friday, 9 a.m. to 9 p.m. Eastern Time (excluding major U.S. holidays). Cherry Health may also be contacted by mail at 100 Cherry Street, SE, Grand Rapids, MI 49501.

Sincerely,
Cherry Health

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/CherryHealth> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. **Please note the deadline to enroll is July 16, 2024.**

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 1-888-964-4694 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

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.

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 <https://www.marylandattorneygeneral.gov>.

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 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.