

NOTICE OF DATA INCIDENT

What Happened?

On June 12, 2026, we became aware of suspicious activity within our email environment after identifying unauthorized logins into one (1) employee email account. Upon discovering this, we promptly initiated an investigation and took steps to identify, contain, and remediate any unauthorized activity. These measures included changing passwords, revoking session tokens, and resetting multifactor authentication. We also engaged experienced data security and privacy professionals to assist in conducting a thorough forensic investigation.

The forensic investigation determined that an unauthorized actor accessed a limited number of emails within a single email account. Due to the swift response of our team, the incident was contained promptly, and no further unauthorized activity was identified.

Through our investigation, we identified that an email containing the personal information of some individuals was potentially accessed by an unauthorized actor. There is currently no evidence that any information has been misused for identity theft or fraud in connection with this incident.

What Information Was Involved?

Based on the findings of the investigation, the following types of information may have been impacted:

- Name
- Phone number
- Date of birth
- Date of service
- Provider name
- Diagnostic and/or treatment information
- Health insurance information

Note that this describes general categories of information identified as present within the accessed email and includes categories that are not relevant to each individual whose information may have been present.

What We Are Doing

We take this incident and the safety of the individuals we serve very seriously.

Upon becoming aware of the incident, we took immediate action to contain the situation and worked closely with data security and privacy professionals to further strengthen our existing, significant safeguards.

After determining that unauthorized activity occurred, we began a thorough analysis of the information involved to identify those potentially affected and notify them. We have also notified the appropriate regulatory authority about this incident.

What Can Impacted Individuals Do?

We encourage individuals to remain attentive to potential identity theft and fraud, regularly monitor reports, review account statements, and report any suspicious activity to the relevant institutions.

Presented below are steps that individuals can take to protect their personal information.

Steps You Can Take to Protect Your Personal Information

Free Credit Report

Under U.S. law, individuals are entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus.

To obtain a free credit report, individuals may visit www.annualcreditreport.com or call toll-free at **1-877-322-8228**.

Alternatively, affected individuals can contact the three (3) major credit reporting bureaus directly at the addresses below:

Equifax PO Box 740241
Atlanta, GA 30374

www.equifax.com
1-800-685-1111

Experian PO Box 2104
Allen, TX 75013

www.experian.com
1-888-397-3742

TransUnion PO Box 2000
Chester, PA 19022

www.transunion.com/data-breach-help
1-833-799-5355

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity.

You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report, please visit www.annualcreditreport.com or call toll-free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form, available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov, to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

Fraud Alert

You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies listed above.

A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but it may also delay you when you seek to obtain credit.

Security Freeze

You may obtain a security freeze on your credit report, free of charge, to protect your privacy and ensure that credit is not granted in your name without your knowledge.

You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft pursuant to the Fair Credit Reporting Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent.

When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or temporarily authorize the release of your credit report to a specific party or parties, or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above.

The following information must be included when requesting a security freeze:

1. Full name, with middle initial and any suffixes;
2. Social Security number;
3. Date of birth;
4. Current address and any previous addresses for the past five (5) years; and
5. Any applicable incident report or complaint with a law enforcement agency or the Department of Motor Vehicles.

The request must also include:

- A copy of a government-issued identification card; and
- A copy of a recent utility bill or bank or insurance statement.

It is essential that each copy be legible and display your name, current mailing address, and the date of issue.

FTC and State Attorney General Offices

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC and/or the Attorney General's office in your home state.

You may also contact these agencies for information on how to prevent or avoid identity theft.

Consumer Response Center — FTC 600 Pennsylvania Avenue, NW
Washington, DC 20580

1-877-IDTHEFT (438-4338)

www.ftc.gov/bcp/edu/microsites/idtheft/

Protecting Medical Information

If you are concerned about protecting your medical information, the following practices can provide additional safeguards to protect against medical identity theft:

- **Protect your health insurance information.** Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- **Review your Explanation of Benefits statements.** Review your "Explanation of Benefits" statement when you receive it from your health insurance company. Follow up with your insurance company or care provider regarding any items you do not recognize. If necessary, contact the care provider listed on the Explanation of Benefits statement and ask for copies of medical records from the date of the potential access (noted above) to the current date.
- **Request a year-to-date services report.** Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider regarding any items you do not recognize.



LOCATIONS

[Community Health Care – Barberton](#)

[Community Health Care – Bergholz](#)

[Community Health Care – Canal Fulton](#)

[Community Health Care – Copley](#)

[Community Health Care – Coventry](#)

[Community Health Care – Louisville](#)

[Community Health Care – Manchester](#)

[Community Health Care - North Canton](#)

[Community Health Care – Wadsworth](#)

[Chippewa Family Medicine - Doylestown](#)

[Community Therapy Center - Physical Therapy](#)

[Green Family Practice - Uniontown](#)

[Hartville Family Physicians - Hartville](#)

[Massillon Family Practice - Massillon](#)

[Norton Family Practice - Norton](#)

[Stow-Kent Family Practice - Stow](#)