# Notice of Data Security Event

Gastro Health is providing notice of phishing incidents that resulted in unauthorized access to certain files and systems. Upon discovery, Gastro Health took immediate action to contain the incident and investigate its scope and impact, which identified certain personal information in the relevant files. Gastro Health is also notifying affected individuals directly, where it has sufficient contact information to do so. Although Gastro Health has no indication at this time that the impacted information has been misused, individuals are encouraged to review this website notice and remain vigilant by reviewing account statements and monitoring credit reports for suspicious activity.

## What Happened?

On February 25, 2026, Gastro Health became aware of a phishing incident involving some of our personnel that resulted in unauthorized access to certain files and systems accessible to those personnel. On March 2, 2026, Gastro Health became aware of a separate phishing incident involving one of our employees that also resulted in unauthorized access to certain files.

## What Information Was Involved?

Impacted data varied by individual and, depending on the individual, may have included: Name, date of birth, Social Security number, government-issued or state-issued ID number, medical record number, patient account number, Medicare or Medicaid number, health insurance or group account number, diagnosis or treatment information, prescription information, and provider or clinic information. No payment card information was impacted in this incident.

## What We Are Doing.

The privacy and security of affected individuals' personal information is important to us. In addition to the actions above, we continue to monitor our systems and continually look for ways to further enhance our information security. Please refer to your notification letter for more information about how to protect your identity, and the resources we are making available.

## What Affected Individuals Can Do.

Regulatory guidance recommends that affected individuals remain vigilant and review personal accounts for suspicious activity. For example, it is beneficial to review: Explanation of Benefit (EOB) letters, Medical records, and account statements and credit reports. We also encourage affected individuals to avoid clicking on links or downloading attachments from suspicious emails and to be cautious of any unsolicited communications that ask for personal information or refer you to a website asking for personal information.

GASTRO HEALTH

## For More Information

We regret any inconvenience or concern this situation may cause. Should affected individuals have questions or concerns, please do not hesitate to contact us at 888-500-5727.

CALL FOR MORE INFORMATION

## Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some steps regulatory agencies recommend you should consider:

### Reviewing Your Accounts and Credit Reports

Regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

| Equifax | Experian | TransUnion |
|---|---|---|
| P.O. Box 105069<br>Atlanta, GA 30348<br>1.800.525.6285<br>Equifax.com | P.O. Box 9554<br>Allen, TX 75013<br>1.888.397.3742<br>Experian.com | P.O. Box 2000<br>Chester, PA 19016<br>1.800.680.7289<br>Transunion.com |

Under federal law, you are entitled to obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com (https://www.annualcreditreport.com). You may also obtain a free report by calling toll free 1.877.322.8228 (tel:+18773228228), or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com (https://www.annualcreditreport.com)) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. If you do not have any free credit reports left, you can still

## Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

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 delay you when you seek to obtain credit. Under federal law, you may place a fraud alert on your file free of charge.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

## Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail: Your full name (including middle initial as well as Jr., Sr., II, III, etc.); social security number; date of birth; the addresses where you have lived over the prior five years; proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; a legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); social security card, pay stub, or W2; and 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. Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing, or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will require you to create or provide you with a credential (such as a PIN number or a password) when you place a security freeze. You will need that credential to lift the freeze and should be careful to record it somewhere secure.

## Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your account or credit reports, or have other reason to believe your information is being misused, you should take the following steps:

File a Police Report. Call your local police office to file a report for identity theft and get a copy of the report to submit to your creditors and others that may require proof of a crime. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf (https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf). The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

**Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New Mexico, New York, North Carolina, Oregon, Rhode Island, and Vermont.**

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at https://oag.dc.gov (https://oag.dc.gov), calling 1.202.727.3400 (tel:+12027273400), or requesting more information via email oag@dc.gov (mailto:oag@dc.gov) or mail 400 6th Street NW, Washington DC 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov (https://www.iowaattorneygeneral.gov), calling 1.515.281.5164 (tel:+15152815164) or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at https://oag.maryland.gov (https://oag.maryland.gov), calling the Identity Theft Unit at 1.410.576.6491 (tel:+14105766491), emailing them at idtheft@oag.state.md.us (mailto:idtheft@oag.state.md.us), or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New Mexico residents are reminded that you have the right to obtain a police report and request a security freeze as described above, and you have rights under the Fair Credit Reporting Act as described above.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the New York State Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft (https://ag.ny.gov/consumer-frauds-bureau/identity-theft); Telephone: 1.800.771.7755 (tel:+18007717755) or the New York Department of State Division of Consumer Protection: https://dos.ny.gov/consumer-protection (https://dos.ny.gov/consumer-protection).

9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us (https://www.doj.state.or.us), calling 1.503.378.4400 (tel:+15033784400) or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by visiting the website at https://riag.ri.gov (https://riag.ri.gov), by phone at 1.401.274.4400 (tel:+14012744400) or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at https://ago.vermont.gov/cap/scam-prevention-through-awareness-and-education/identity-theft (https://ago.vermont.gov/cap/scam-prevention-through-awareness-and-education/identity-theft).

**Gastro Health Support Center**
9200 S. Dadeland Blvd.
Suite 800
Miami, FL 33156

GASTRO HEALTH

**Careers**
**Employees**
**Gastro Health Foundation**