

Gastroenterology Consultants of South Texas Provides Notice of Data Incident

This notice is from Gastroenterology Consultants of South Texas (“GCST,” “we,” “us,” or “our”) about a recent security incident. GCST is a gastroenterology, colorectal and foregut surgery practice specializing in digestive health in South Texas.

GCST is posting this substitute notice to provide customers and individuals with information about the cybersecurity incident on GCST’s systems and to share resources available to people whose personal data may have been impacted.

The review of potential personal information that may have been involved in this incident is now complete. GCST is providing this notice to help potentially impacted individuals understand what happened, let them know what information may have been impacted, and give them information on steps they can take to protect their privacy.

This substitute notice contains the information GCST can provide at this time. GCST has identified potentially affected individuals and is mailing written letters to those individuals for whom we have a sufficient address. Please note, we may not have sufficient addresses for all affected individuals.

What Happened? GCST detected unauthorized activity in our information technology (IT) systems. Upon discovering this activity, we immediately took protective actions to stop the unauthorized access, notified U.S. federal law enforcement, and launched an investigation with the assistance of leading cybersecurity specialists. The investigation indicated that some personal information may have been accessed by an unauthorized party in late May 2025. At this time, we have no reason to believe your information has been misused; however, we are providing you notice out of an abundance of caution.

What Personal Information May Be Involved? The information varied by patient but could have included protected health information.

What We Are Doing. We are taking this incident very seriously. Upon detecting unauthorized activity in our IT systems, we took immediate protective actions to contain the activity and retained industry-leading cybersecurity specialists to investigate the incident, ensure the unauthorized access ceased, and use lessons learned to improve our systems’ security posture. Individuals potentially affected by this incident are being offered free credit monitoring by TransUnion. Affected individuals also are encouraged to remain vigilant and monitor their account statements, bills, notices, financial transactions, and free credit reports for potential fraud and identity theft, and to promptly report any questionable or suspicious activity. If you have questions regarding this incident or the services available to you, please call 1-800-405-6108 (excluding major U.S. Holidays): *Central Time*: Monday to Friday 7:00 AM to 7:00 PM. To help prevent a similar incident from happening in the future, Vendor is further enhancing workforce training, among other measures.

Sincerely,

Recommended Steps to Help Protect Your Information

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.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Place Fraud Alerts with the Three Credit Bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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 also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com	Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000 www.transunion.com
--	--	--

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files. This can be accomplished by contacting the credit bureaus listed below:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Additional Information. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Texas Residents: Visit the Texas Attorney General Office (<https://www.texasattorneygeneral.gov/consumer-protection/identity-theft>) for additional information on protection against identity theft.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.