

May 30, 2024

Dominik Cvitanovic
(504)-702-1710

Dominik.Cvitanovic@wilsonelser.com

Via E-Mail: Idtheft@oag.state.md.us

Attorney General Anthony Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Cybersecurity Incident

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Gastroenterology Associates of Central Florida, P.A. dba Center for Digestive Health (“Gastroenterology Associates”), a medical practice located in Orlando, Florida, with respect to a recent cybersecurity incident that was first discovered by Gastroenterology Associates on May 7, 2024 (hereinafter, the “Incident”). Gastroenterology Associates takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that Gastroenterology Associates has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On April 11, 2024, Gastroenterology Associates detected suspicious activity in its network environment. Upon discovery of this incident, Gastroenterology Associates promptly took steps to secure its network environment and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident.

Gastroenterology Associates immediately began a thorough review of the potentially accessed files to identify the clients whose sensitive information was present at the time of the Incident. This step was necessary so that Gastroenterology Associates could send a notice of the Incident to ensure

the potentially impacted individuals are aware of this Incident. On May 7, 2024, the investigation identified persons whose sensitive information may have been accessed. The identified PII included name, Social Security number, and limited financial information.

Gastroenterology Associates has secured and remediated its network environment and the data that it maintains. As of this writing, Gastroenterology Associates has not received any reports of related identity theft since the date of the incident.

2. Number of Maryland residents affected.

One Maryland resident may have been potentially affected by this incident. A notification letter to this individual was mailed on May 29, 2024, by first-class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate an investigation to identify potentially affected individuals. We retained a leading data privacy and cybersecurity firm that assisted in investigating and confirming the security of our systems. We promptly reset passwords for all accounts and isolated the network. We also deployed additional monitoring tools and will continue to enhance the security of our systems.

Although Gastroenterology Associates is not aware of any actual or attempted misuse of the affected personal information, Gastroenterology Associates offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through TransUnion to all individuals to help protect their identity. Additionally, Gastroenterology Associates provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

Gastroenterology Associates remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at dominik.cvitanovic@wilsonelser.com or 504-372-6698.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Dominik J. Cvitanovic, Esq.

EXHIBIT A

Gastroenterology Associates of Central Florida, P.A.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08907 5-3



Henry Levine M.D., F.A.C.P., A.G.A.F.
William Mayoral M.D.
Marlon Ilagan M.D.
Samuel Giday M.D.
Jason Korenblit M.D.
Ehsan Rafiq M.D.

Via First-Class Mail



May 29, 2024

Dear _____ :

Gastroenterology Associates of Central Florida, P.A. (“Gastroenterology Associates”) is writing to inform you of a recent data security incident that has resulted in unauthorized access to your data. While we are unaware of any fraudulent misuse of your data at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your data. Please be assured Gastroenterology Associates takes the protection and proper use of your data very seriously.

What Happened?

In recent days Gastroenterology Associates has detected suspicious activity in its IT network environment. Upon discovery of this incident, Gastroenterology Associates promptly took steps to secure its network environment and engaged a specialized cybersecurity firm to investigate the nature and scope of the incident. As a result of the investigation, Gastroenterology Associates learned that an unauthorized actor accessed certain files and data stored within our network, as has occurred in many other businesses, banks, and large corporations in America.

Gastroenterology Associates’ forensic investigator determined that an unauthorized third party accessed its network environment between April 1 and 14, 2024. Upon learning this, Gastroenterology Associates launched a review of the potentially affected data to identify the individuals and information involved. On May 7, 2024, Gastroenterology Associates identified persons whose personal identifiable information (“PII”) was included within the impacted data. At this time, we have no evidence any of the information has been misused by a third party, but because information related to you was disclosed, we are notifying you out of full transparency.

What Information Was Involved?

The following data was accessed by a person not authorized to view them: name, Social Security number, and limited financial information.

What We Are Doing?

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate an investigation, which included retaining a leading forensic investigation firm who assisted in conducting an investigation and confirming the security of our network environment. We also deployed additional monitoring tools and will continue to enhance the security of our systems. We take the protection and proper use of personal information very seriously.

As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident, and we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **9453E72F E3**. Please note that the code is case-sensitive and will need to be entered as it appears.

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have 12 months of monitoring services. At the end of 12 months, the services will be deactivated. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

Representatives of Cyberscout are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line 1-800-405-6108 and supply the fraud specialist with the unique code listed above. The call center representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Gastroenterology Associates sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Gastroenterology Associates of Central Florida, P.A.
dba Center for Digestive Health

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (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 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf));
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a 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.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.