

August 9, 2021

**Robert Walker**  
601.499.8083 (direct)  
Robert.Walker@wilsonelser.com

Via Online Portal

**Attorney General Aaron Frey**  
Office of the Attorney General  
6 State House Station  
Augusta, ME 04333

Notice of Data Breach

---

**Re: Our Client : Gastroenterology Consultants, P.A.**  
**Matter : Data Security Incident on January 10, 2021**  
**Wilson Elser File # : 16516.01306**

---

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Gastroenterology Consultants, P.A. (“Gastroenterology”), a comprehensive gastrointestinal health care provider located in 444 FM 1959, Suite A, Houston, Texas 77034 and five other locations, with respect to a data security incident that was first discovered by Gastroenterology on January 10, 2021 (hereinafter, the “Incident”). Gastroenterology 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 Maine residents being notified, and the steps that Gastroenterology 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 January 10, 2021, Gastroenterology experienced a data security incident involving a ransomware virus which resulted in the potential exposure of our employees’ personal information to an unauthorized individual. Upon discovery of the attack, Gastroenterology promptly engaged a specialized cybersecurity firm and breach counsel to conduct a forensic investigation to determine the nature and scope of the incident. The investigation indicated some files containing sensitive personal information may have been exfiltrated by the attacker. However, based on the negotiated resolution with the attacker, Gastroenterology received assurances that any potential exfiltrated data had been destroyed. Gastroenterology then promptly performed data mining to identify the specific individuals and the type of information that may have been compromised.

This step was necessary so that Gastroenterology could send a notice of the incident to ensure the potentially impacted individuals are aware of the incident.

Although Gastroenterology is unaware of any fraudulent misuse of information, it is possible that individuals' full name, address, and Social Security number may have been exposed as a result of this unauthorized activity.

As of this writing, Gastroenterology has not received any reports of related identity theft since the date of the incident (January 10, 2021 to present).

## **2. Number of Maine residents affected.**

Gastroenterology identified and notified 162,163 individuals potentially affected by this Incident. Of those, one (1) was a resident of Maine. Notification letter to this individual was mailed on August 6, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

## **3. Steps taken in response to the Incident.**

Gastroenterology is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Gastroenterology moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. Specifically, Gastroenterology engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, Gastroenterology deployed endpoint monitoring and detection tools to continuously monitor for any malicious activity within its systems. Lastly, Gastroenterology informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although Gastroenterology is not aware of any actual or attempted misuse of the affected personal information, Gastroenterology offered 12 months of complimentary credit monitoring and identity theft restoration services through IDX to all individuals to help protect their identity. Additionally, Gastroenterology 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 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 [Robert.Walker@wilsonelser.com](mailto:Robert.Walker@wilsonelser.com) or 601-499-8083.



Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**

A handwritten signature in blue ink, appearing to read 'Robert Walker'.

Robert Walker, Esq.

Copy: Wilson Elser LLP  
Attn: Mary H. Park, Esq.

Enclosure: *Sample Notification Letter*



PO Box 4129  
Everett WA 98204

ENDORSE



NAME  
ADDRESS1  
ADDRESS2  
CSZ  
COUNTRY

BREAK

To Enroll, Please Call:  
(833) 909-3925  
Or Visit:

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

Enrollment Code: <<XXXXXXXXXX>>

August 6, 2021



SEQ  
CODE 2D  
Ver 2ES

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

Gastroenterology Consultants, P.A. (“Gastroenterology”) is writing to inform you of a recent data security incident that may have resulted in an unauthorized access of your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the event, steps we are taking in response, and resources available to help you protect against the misuse of your information.

**What Happened?** On January 10, 2021, Gastroenterology experienced a data security incident involving a ransomware virus which resulted in the potential exposure of our employees’ personal information to an unauthorized individual. Upon discovery of the attack, Gastroenterology promptly engaged a specialized cybersecurity firm and breach counsel to conduct a forensic investigation to determine the nature and scope of the incident. The investigation indicated some files containing sensitive personal information may have been exfiltrated by the attacker. However, based on our negotiated resolution with the attacker, we received assurances that any potential exfiltrated data had been destroyed. Gastroenterology promptly performed data mining to identify the specific individuals and the type of information that may have been compromised. This step was necessary so that we could identify the affected population in order to send out notice of the incident to these individuals. At this time, there has been no evidence that any sensitive data has been used in any unauthorized manner.

**What Information Was Involved?** The types of information impacted varied by individual. However, the information present during the period of unauthorized access may have included your name, address, and social security number.

**What We Are Doing** We are committed to doing everything we can to help protect the privacy and security of the personal information in our care. Since the discovery of the incident, we have taken and will continue to take steps to mitigate the risk of future issues. Notably, we launched an investigation to determine the full nature and scope of this incident. Additionally, we deployed endpoint monitoring and detection tools to continuously monitor for any malicious activity within our systems. We are also providing you with guidance on how to help protect against the possibility of information misuse.

Out of an abundance of caution, we are providing you with 12 months of complimentary credit monitoring services through IDX. While we are covering the cost of these services, you will need to complete the activation process by following the instructions included in the enclosed *Steps You Can Take to Help Protect Your Information*.

Again, based on available evidence through monitoring, we are not aware of your information being used in an unauthorized manner, but out of an abundance of caution, we wanted to inform you of this incident.

**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.

You may also activate the credit monitoring services we are making available to you. Again, we are making these services available to you at no cost; however, you will need to activate yourself in these services. The deadline to enroll is November 6, 2021.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

**For More Information** We recognize that you may have questions not addressed in this letter. If you have additional questions, please call (833) 909-3925 (toll free) during the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday, (excluding U.S. national holidays) or email us at [potential\\_databreach\\_questions@gastroconsultants.com](mailto:potential_databreach_questions@gastroconsultants.com).

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

Sincerely,

A handwritten signature in black ink that reads "Nita James R.N." in a cursive script.

Nita James  
Gastroenterology Consultants, P.A.

## Steps You Can Take to Help Protect Your Information

### Enroll in Credit Monitoring Services

- 1. Website and Enrollment.** Go to <https://response.idx.us/services> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 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 (833) 909-3925 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

### Additional Important Information

#### For residents of all states:

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

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

#### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

#### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-888-525-6285

<https://www.equifax.com/personal/cred>

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

**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:

#### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

More information can also be obtained by contacting the Federal Trade Commission:

**Federal Trade Commission** - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); [www.identitytheft.gov](http://www.identitytheft.gov).

**For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming:** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

**For residents of Colorado, Illinois, Iowa, Maryland, Missouri, New Mexico, North Carolina, Oregon, and West Virginia:** It is required by state laws to inform you that 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](http://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.

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For residents of New Mexico:** State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach.

**For residents of Massachusetts:** 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 residents of Oregon:** State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

**For residents of Rhode Island:** It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

**For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Federal Trade Commission - Consumer Response Center:** 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); [www.identitytheft.gov](http://www.identitytheft.gov)

**Arizona Office of the Attorney General Consumer Protection & Advocacy Section,** 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

**Colorado Office of the Attorney General Consumer Protection** 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 [www.coag.gov](http://www.coag.gov)

**District of Columbia Office of the Attorney General – Office of Consumer Protection:** 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov)

**Illinois office of the Attorney General -** 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**Maryland Office of the Attorney General - Consumer Protection Division:** 200 St. Paul Place, 16<sup>th</sup> floor, Baltimore, MD 21202; 1-888-743-0023; [www.oag.state.md.us](http://www.oag.state.md.us)

**New York Office of Attorney General - Consumer Frauds & Protection:** The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

**North Carolina Office of the Attorney General - Consumer Protection Division:** 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; [www.ncdoj.com](http://www.ncdoj.com)

**Rhode Island Office of the Attorney General - Consumer Protection:** 150 South Main St., Providence RI 02903; 1-401-274-4400; [www.riag.ri.gov](http://www.riag.ri.gov)