

11 South Meridian Street
Indianapolis, IN 46204-3535
U.S.A.
(317) 236-1313
Fax (317) 231-7433
www.btlaw.com

Stacy L. Cook
Partner
317-231-7237
scook@btlaw.com

Via Email Only to Idtheft@oag.state.md.us

March 29, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Notice of Incident

Dear Sir/Madam:

We are writing to notify you of a security incident on behalf of our client, Otolaryngology Associates LLC (“OA”) located in central Indiana. Maryland residents may have been impacted by the security incident.

On February 17, 2024, through alerts on its systems, OA became aware that it was the victim of a criminal cyber-attack. OA promptly took steps to secure its information systems and investigate the incident, including contacting the FBI and hiring a forensic cybersecurity firm, to try to determine which, if any, information was accessed or stolen. As a result of the investigation, on March 5, 2024, it was ultimately determined that the attacker did not view individual documents, but ran programs to exfiltrate (take) some data from OA systems; therefore OA is notifying all potentially affected individuals of the incident.

The data involved included first and last name, OA medical record number, a code related to the services provided, date(s) of service, treating physician name, appointment location, dollar amount of charges and name of insurance company and Social Security number and/or driver’s license number. For some individuals other information could include address, email address, telephone number, date of birth, appointment schedules, referral forms, or insurance plan numbers. The attacker did not gain access to OA’s electronic patient health records. The vast majority of impacted individuals did not have their Social Security number or driver’s license number exposed. OA continues to pursue measures to protect and secure its data. No Maryland residents had their Social Security number or driver’s license number impacted.

OA will be mailing the attached notification letter to twenty-four (24) Maryland residents in the next few days.

Please contact me at scook@btlaw.com or 317-231-7237 if you have any questions or request additional information.

Best regards,

A handwritten signature in blue ink, appearing to read 'SLC', is positioned above the printed name.

Stacy L. Cook
Barnes & Thornburg LLP

Enclosure: Notifications to Affected Individuals

<<Date>> (Format: Month Day, Year)

Parent or Guardian of

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>

<<address_1>>

<<address_2>>

<<city>>, <<state_province>> <<postal_code>>

<<country>>

Notice of Data Breach

Dear Parent or Guardian of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Otolaryngology Associates LLC (“OA”) is sending you this letter to notify you of a recent incident which may have involved your child’s Protected Health Information (“PHI”). We take the protection and proper use of information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On February 17, 2024, through alerts on its systems, OA became aware that we were the victim of a criminal cyber-attack. OA discovered the attack within hours after it began and OA’s vendor took immediate steps to try to stop the attack. OA has had continuous access to its systems and was never locked out of its systems. On February 20 and 21, 2024, the attacker sent three communications claiming to have stolen some of our data and threatening to release the stolen data publicly. We promptly took steps to further secure our information systems and investigate the incident, including contacting the FBI and hiring a forensic cybersecurity firm. As a result of the investigation, it was ultimately determined that the attacker did not view individual documents, but ran programs to exfiltrate (take) some data from OA systems. While the investigation narrowed down which data might have been taken, it could not definitively determine which specific documents in that subset of data may have been taken. As a result, OA could not rule out the possibility that your child’s information may have been compromised. OA continues to monitor the situation closely.

What information was involved?

The attacker did not gain access to OA’s electronic patient health records. Neither your child’s Social Security number nor driver’s license number were impacted by this attack. PHI that may have been impacted includes some billing information such as: first and last name, OA medical record number, a code related to the services provided, date(s) of service, treating physician name, appointment location, dollar amount of charges and name of insurance company. For some individuals other information could include address, email address, telephone number, date of birth, appointment schedules, referral forms.

What we are doing.

OA takes the protection of your child’s PHI seriously. In addition to engaging a cybersecurity firm to ensure protection of our systems and investigate the incident, OA promptly took (and continues to take) other actions to further protect its patients and systems post-incident, including implementing additional security measures.

What you can do.

Please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect your child’s identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your child’s credit file.

For more information.

If you have questions, please call [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

John D. Goldenberg, MD

President

Otolaryngology Associates, LLC

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

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 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three 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.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys 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 Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Otolaryngology Associates LLC (“OA”) is sending you this letter to notify you of a recent incident which may have involved your Protected Health Information (“PHI”). We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On February 17, 2024, through alerts on its systems, OA became aware that we were the victim of a criminal cyber-attack. OA discovered the attack within hours after it began and OA’s vendor took immediate steps to try to stop the attack. OA has had continuous access to its systems and was never locked out of its systems. On February 20 and 21, 2024, the attacker sent three communications claiming to have stolen some of our data and threatening to release the stolen data publicly. We promptly took steps to further secure our information systems and investigate the incident, including contacting the FBI and hiring a forensic cybersecurity firm. As a result of the investigation, it was ultimately determined that the attacker did not view individual documents, but ran programs to exfiltrate (take) some data from OA systems. While the investigation narrowed down which data might have been taken, it could not definitively determine which specific documents in that subset of data may have been taken. As a result, OA could not rule out the possibility that your information may have been compromised. OA continues to monitor the situation closely.

What information was involved?

The attacker did not gain access to OA’s electronic patient health records. Neither your Social Security number nor your driver’s license number were impacted by this attack. PHI that may have been impacted includes some billing information such as: first and last name, OA medical record number, a code related to the services provided, date(s) of service, treating physician name, appointment location, dollar amount of charges and name of insurance company. For some individuals other information could include address, email address, telephone number, date of birth, appointment schedules, referral forms.

What we are doing.

OA takes the protection of your PHI seriously. In addition to engaging a cybersecurity firm to ensure protection of our systems and investigate the incident, OA promptly took (and continues to take) other actions to further protect its patients and systems post-incident, including implementing additional security measures.

What you can do.

Please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call [TFN](#), Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

John D. Goldenberg, MD

President

Otolaryngology Associates, LLC

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

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 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three 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.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys 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 Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.