17794

Atlantic Medical Imaging

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Atlantic Medical Imaging ("AMI") writes to inform you of a security incident that occurred between September 6, 2019 and September 16, 2019. While there is currently no evidence that any personal information has been compromised or misused as a result of this incident, out of an abundance of caution, we are providing you with information about the incident, our response to it, and resources available to you to better protect your information, should you feel it appropriate to do so.

What Happened? AMI became aware of unusual activity involving certain employee email accounts. AMI immediately commenced an investigation with the assistance of third-party computer specialists. The investigation determined that certain employee email accounts were accessed without authorization between September 6, 2019 and September 16, 2019. While the investigation did not determine that any personal information had actually been viewed by an unauthorized actor, AMI could not rule out the possibility of such activity. Therefore, AMI, through third party forensic specialists, conducted a thorough review of the complete contents of the email accounts to determine whether sensitive information was present in the accounts at the time of the incident.

AMI received the preliminary results of the investigation which indicated that personal information may have been present in the affected email accounts and to whom that information pertained at the time of the incident on August 22, 2020. On August 25, 2020, AMI completed its review of this information and our files to determine the identities of those who were potentially involved and their last known address information for purposes of notifying them of this incident. Through this process, we determined that your personal information was present in an affected email account at the time of the incident. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

What Information Was Involved? Our investigation determined that at the time of the incident the email accounts contained information including your name and <<Data Elements>>.

What Are We Doing. Information, privacy, and security are among our highest priorities. AMI has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for AMI email accounts, implemented increased security measures for email account access, conducted additional employee training, hired an outside security operations center (SOC) to do 24/7 monitoring for any malware or suspicious activity, and thoroughly reviewed and updated policies and procedures relating to data security. We also provided relevant regulatory notices, including notice to the Department of Health and Human Services.

While, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident, we are notifying you so that you may take further steps to better protect your personal information should you feel it is appropriate to do so. We also secured the services of Experian to provide identity and credit monitoring services at no cost to you for <<CM Length>> months. For more information on these services, please review below.

Experian credit monitoring services are for <<CM Length>> months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have.

To enroll in Credit Monitoring* services at no charge, please log on to https://www.myidmanager.com and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Activation Code>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What Can You Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, review your Explanation of Benefits form, and to monitor your credit reports for suspicious activity for the next twelve (12) to twenty-four (24) months. You may review the information contained in the attached "Steps You Can Take to Help Protect Your Information." You may also enroll to receive the identity and credit monitoring services we are making available to you as we are unable to enroll in these services on your behalf.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 888-905-0122 (toll free), Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time. You may also contact Atlantic Medical Imaging by mail at 72 W. Jimmie Leeds Road STE. 1100, Galloway, NJ 08205.

Atlantic Medical Imaging takes the privacy and security of the personal information in our care seriously. Please let us know if you have any questions.

Sincerely,

David Levi, M.D.
Atlantic Medical Imaging

Steps You Can Take to Help Protect Your Information

Monitor Accounts

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 activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

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 and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft. ***For Maryland residents***, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; or www.oag.state.md.us. Atlantic Medical Imaging may be contacted by mail at 72 W. Jimmie Leeds Road STE. 1100, Galloway, NJ 08205. ***For New Mexico residents***, individuals have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in the individual's credit file has been used against the individual, the right to know what is in an individual's credit file, the right to ask for an individual's credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to an individual's file is limited; an individual must give consent for credit reports to be provided to employers; an individual may limit "prescreened" offers of credit and insurance an individual would get based on information in a credit report; and an individual may seek damages from violators. An individual may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage individuals to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580. ***For Rhode Island residents***, The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; or 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident. ***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/.