Radiologic Medical Services, PC

Radiologic Medical Services, PC c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

October 6, 2025

Dear [REDACTED]:

We write to inform you of a data security incident experienced by Radiologic Medical Services, P.C. that may have involved your information as described below. We take the privacy and security of all information very seriously and are providing information about the incident and steps you can take to help protect your information.

What Happened: On February 26, 2024, we discovered suspicious activity related to an employee email account. Upon discovery, we took immediate action to address and investigate the incident, which included engaging third-party specialists to assist with determining the nature and scope of the incident. A thorough investigation determined that two employee email accounts were subject to unauthorized access from February 22, 2024, through March 19, 2024. We then began a thorough review of the contents of the accounts in order to determine the type(s) of information contained within the accounts and to whom that information related. Once this review was completed, we worked to obtain up-to-date address information in order to provide you with this notice. That process was completed on September 13, 2024, and we worked to provide you with this notification as soon as possible.

What Information Was Involved: The types of information that may have been contained within the affected data includes your first and last name, in combination with [REDACTED]. Please note that we currently have no reason to believe that your information has been or will be misused as a result of this incident.

What We Are Doing: We have taken the steps necessary to address the incident and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately took steps to secure the email accounts and undertook a thorough investigation. We have also implemented additional technical safeguards to further enhance the security of information in our possession and to prevent similar incidents from happening in the future. Additionally, we are offering you complimentary credit monitoring and identity protection services.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports, account statements, and explanation of benefits documents for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, including activating the complimentary credit monitoring and identity protection services we are offering.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line which can be reached at [REDACTED].

Sincerely,

Carrie Cole

Carrie Cole
Business Manager

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Credit Monitoring Instructions

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit 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 credit freeze 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 credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1-800-680-7289	1-888-397-3742	1-888-298-0045
www.transunion.com	www.experian.com	www.equifax.com
TransUnion Fraud Alert	**Experian Fraud Alert**	**Equifax Fraud Alert**
P.O. Box 2000	P.O. Box 9554	P.O. Box 105069
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30348-5069
TransUnion Credit Freeze	**Experian Credit Freeze**	**Equifax Credit Freeze**
P.O. Box 160	P.O. Box 9554	P.O. Box 105788
Woodlyn, PA 19094	Allen, TX 75013	Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. Radiologic Medical Services, P.C. may be contacted at 2669 Heartland Drive, Suite #105, Coralville, IA 52241.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and https://oag.dc.gov/consumer-protection. Radiologic Medical Services, P.C. may be contacted at 2669 Heartland Drive, Suite #105, Coralville, IA 52241.