Radiology Chartered
c/o Return Processing Center
P.O. Box 3826
Suwanee, GA 30024

Via First-Class Mail

1 1 26 *******************AUTO**MIXED AADC 302
[redacted]

May 16, 2025

RE: Notice of Data Event

Dear [redacted]:

Radiology Chartered writes to inform you regarding a recent incident, which may impact the security of some of your personal information. The incident occurred at Nationwide Recovery Services, Inc. ("NRS"), which Radiology Chartered, previously known as Computer Scanning Services and CT Imaging LLC, used in the past as a third-party vendor for various services, including payment collection. Radiology Chartered was in no way directly involved in this incident and NRS likely received your information in the past in furtherance of services rendered to Radiology Chartered.

Radiology Chartered treats this event with the utmost seriousness, and the privacy, security, and confidentiality with which vendors treat our patients' information is among our highest priorities. While we are not aware of any actual or attempted misuse of your information, out of an abundance of caution, we are providing you with this notice, informing you of what occurred, our response, and resources to help further protect your information, should you feel it necessary to do so.

<u>What Happened?</u>

On or around March 24, 2025, Radiology Chartered received written notice from NRS regarding the incident. On July 11, 2024, NRS became aware of a cybersecurity issue involving its network environment. NRS's investigation into the issue determined that an unknown actor had gained unauthorized access to systems on NRS's network from July 5, 2024 to July 11, 2024. During this time, the unknown actor copied files that were stored on one system. NRS did not inform Radiology Chartered of the extent of the incident's impact until after March 20, 2025, when NRS mailed the notice that the incident may have impacted the security of personal information relating to certain Radiology Chartered patients. Radiology Chartered had no knowledge of any impact to individuals prior to this notice from NRS nor was Radiology Chartered aware that data previously provided to NRS was still in NRS's possession.

Upon receiving the notice from NRS, we promptly commenced an extensive review to remove duplicated individuals and identify missing address information necessary to notify all potentially affected individuals.

<u>What Information Was Involved?</u>

While NRS's investigation could not conclusively determine the specific information involved for each individual, the following types of personal information relating to you may have potentially been present within the impacted data: name, Social Security number, and date of birth.

What We Are Doing.

As stated above, the privacy, security, and confidentiality with which vendors treat our patient's information is among our highest priorities. Upon receiving notice from NRS of this incident's impact, we promptly moved to review the information and individuals potentially involved. While we are not aware of any actual or attempted misuse of your information, we are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We are also notifying the Department of Health of Human Services of this incident.

As an added precaution, we are providing you with access to credit monitoring and identity protection 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. These alerts are 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 HaystackID, which specializes in fraud assistance and remediation services. While Radiology Chartered is covering the cost of these services, you will need to complete the activation process yourself.

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 Personal Information*, to learn more about how to protect against potential information misuse.

To enroll in Credit Monitoring services at no charge, please log on to www.privacysolutions.com and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. 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 by August 13, 2025. 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, after which 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.

We apologize for any inconvenience this incident may cause. We share your frustration and hope for your understanding. If you have questions or are unable to activate credit monitoring according to the enclosed instructions, please call the dedicated assistance line at 855-260-7977, Monday through Friday from 9:00a.m. to 9:00p.m. Eastern Time, excluding major U.S. holidays. Please have this letter ready if you call.

Sincerely,

Radiology Chartered

Steps You Can Take To Help Protect Personal Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877¬322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Consumers who wish to place a credit freeze or fraud alert should contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/ credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above.

Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, consumers will likely need to provide proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Maryland residents, you may also wish to review information from the Maryland Attorney General on how to avoid identity theft at www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491. Radiology Chartered is located at 1789 Shawano Ave, Green Bay, WI 54303 and can be reached at 920-499-1428.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; 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 under the Fair Credit Reporting Act at 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 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/.

For Rhode Island residents, this data event involves 1 individual in Rhode Island. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.