



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

SEP 18 2022

CONSUMER PROTECTION

Elizabeth Dill
Office: (267) 930-5327
Fax: (267) 930-4771
Email: edill@mullen.law

4870 Sadler Road, Suite 300
Glen Allen, VA 23060

September 9, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We continue to represent Radiology Associates of Albuquerque and Advanced Imaging, LLC, (together, "RAA"), located at 4411 The 25 Way, Suite 150, Albuquerque, NM 87109, and write to supplement our July 28, 2022 notification to your office regarding an incident that may affect certain personal information relating to New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, RAA does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Per our prior notification to your office, in August 2021, RAA learned that it experienced a cyber incident. RAA promptly took steps to secure its systems and commenced an investigation into the nature and scope of the incident. RAA has been working diligently to investigate this incident and confirm any information that may be affected. Through the investigation, it was determined that certain documents stored within RAA's environment were copied from the system as part of the cyber incident between July 22, 2021 and August 3, 2021. Through the investigation, RAA further determined that certain email accounts were accessed without authorization at varying times between December 22, 2020 and July 15, 2021. Based on the investigation, RAA conducted a detailed review of the potentially impacted data to determine the type of information present and to whom it related. This process to review and catalogue the data and determine whose information may be affected has been ongoing and, in relation to patients of RAA correlated to a specific healthcare facility, was recently completed on or around July 16, 2022. Through address validation efforts, on August 29, 2022, RAA confirmed that additional New Hampshire residents were potentially affected by this incident. RAA is now working to provide further notice to those individuals whose information may be affected.

Mullen.law

The personal information, as defined by N.H. Rev. Stat. Ann. § 359-C:19, that may be affected includes: name and Social Security number.

Notice to New Hampshire Residents

Per our prior notification to your office, on July 28, 2022, RAA began providing notice to potentially affected New Hampshire residents. Based on the data review efforts discussed above, on September 9, 2022, RAA will be providing written notice to an additional sixty-five (65) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***. Previously, in October 2021, while its investigation was ongoing, RAA posted notice of this incident to its website and provided notice to statewide media in New Mexico. On July 28, 2022, RAA updated the notice provided on its website and also provided notice to media in all 50 U.S. states.

Other Steps Taken and To Be Taken

The confidentiality, privacy, and security of information within its care are among RAA's highest priorities. Upon learning of the event, RAA promptly took steps to secure its systems and investigate the full scope of the incident. While the response to the incident is ongoing, RAA has taken additional steps to further enhance the security of its systems. RAA is also notifying potentially affected individuals and providing information on steps they may take to best protect their information, including providing individuals with 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 encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud. RAA is also offering affected individuals access to 24 months of credit monitoring and identity theft protection at no cost to the individual. Further, RAA has reported this incident to the Federal Bureau of Investigation and the U.S. Department of Health and Human Services ("HHS"), and will be reporting the incident to other state regulatory authorities and consumer reporting agencies as appropriate.

Contact Information

Should you have any questions regarding this notification, please contact us at (267) 930-5327.

Very truly yours,

Elizabeth Dill of
MULLEN COUGHLIN LLC

ERD/ajl
Enclosure

2022 SEP 13 PM 1:14
STATE OF NH
DEPT OF JUSTICE

EXHIBIT A



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

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

<<b2b_text_1(Subject Line)>>

Dear <<First_Name>> <<Last_Name>>,

Radiology Associates of Albuquerque, also known as RAA Imaging, and Advanced Imaging, LLC, also known as High Resolution, (together "RAA") are writing to make you aware of an incident that may affect your personal information. We want to provide you with information about the incident, our response, and steps you may take to protect your personal information, should you feel it appropriate to do so. RAA is a radiological services provider whose radiologists provide services at a hospital or clinic you visited.

What Happened? In August 2021, RAA learned that it experienced a cyber incident. We promptly took steps to secure our systems and commenced an investigation into the nature and scope of the incident. We have been working diligently to investigate this incident and confirm any information that may be affected. Through the investigation, we determined that certain documents stored within RAA's environment were copied from the system as part of the cyber incident between July 22, 2021 and August 3, 2021. The investigation further determined that certain email accounts were accessed without authorization at varying times between December 22, 2020 and July 15, 2021. Based on the investigation, RAA conducted a detailed review of data involved to determine the type of information present and to whom it related. For certain patient information, this process to review the data and determine whose information may be affected has been ongoing and was preliminarily completed in July 2022. RAA then undertook a detailed effort to reconcile and consolidate the information in order to identify specific individual and contact information. You are receiving this notice because we determined that your information may be affected.

What Information Was Involved? The personal information potentially affected varies by individual. It may include: name, Social Security number, date of birth, patient identification number, billing information, and exam type.

What We Are Doing. The confidentiality, privacy, and security of information within our care are among RAA's highest priorities. Upon learning of the event, we promptly took steps to secure our systems and investigate the full scope of the incident. While our investigation of and response to the event are ongoing, we have taken additional steps to further enhance the security of our systems. In an abundance of caution, we are also notifying potentially affected individuals, including you, and providing information on steps you may take to best protect your information, should you feel it is appropriate to do so. We are also offering you access to identity monitoring at no cost to you as an added precaution. Information on how to activate these services may be found in the attached "*Steps You Can Take to Help Protect Personal Information*."

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefit forms and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the information contained in the attached "*Steps You Can Take to Help Protect Personal Information*" and to activate the identity monitoring services we are making available to you.

For More Information. If you have additional questions, please call our dedicated assistance line at (855) 516-3877, Monday-Friday: 7:00 am-4:30 pm Mountain Time, excluding major U.S. holidays.

Sincerely,

**Radiology Associates of Albuquerque, PA
Advanced Imaging, LLC**

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate Identity Monitoring

We have secured the services of Kroll to provide identity monitoring at no cost to you for two (2) years. Kroll is a global leader in risk mitigation and response. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number (S_N)>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, please 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
888-298-0045	1-888-397-3742	833-395-6938
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. 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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. 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 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, the consumer reporting bureaus 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 violator. 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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. RAA is located at 4411 The 25 Way, Ste. 150, Albuquerque, NM 87109.

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 reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 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 31 Rhode Island residents impacted by this incident.