



LEWIS BRISBOIS BISGAARD & SMITH LLP

Erica Lloyd
601.499.8127 (direct)
Erica.Lloyd@lewisbrisbois.com

August 14, 2023

Via Electronic Mail: *Idtheft@oag.state.md.us*

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

Re: Client : TRACT Radiology
Matter : Data Security Incident

Dear Attorney General:

We are writing on behalf of TRACT Radiology with respect to a potential data security incident described in more detail below. TRACT Radiology takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of Maryland residents that were potentially affected, what information has been compromised, and the steps that TRACT Radiology is taking to secure the integrity of its systems. We have also enclosed hereto samples of the notifications made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

TRACT Radiology, is a medical business office located in Tulsa, Oklahoma which provides billing and administrative services to two physician group practices, Tulsa Radiology Associates and Radiology Consultants of Tulsa. TRACT Radiology stores all data for its affiliates.

On the morning of July 9, 2023, TRACT Radiology, was the victim of a ransomware incident. Upon discovery of the Incident, TRACT Radiology immediately engaged third-party forensic specialists to assist us with securing the network environment and investigating the extent of any unauthorized activity. The forensic investigation, which concluded on August 3, 2023,

determined an unauthorized third party may have acquired certain individual personal and health information during this incident.

Although TRACT Radiology is not aware of any evidence of misuse of personal information, TRACT Radiology is notifying and extending an offer for free credit monitoring and identity theft protection through Sontiq to all potentially impacted individuals. This service will include 12-24 months of credit monitoring, along with fully managed ID theft recover service, should the need arise.

As of this writing, TRACT Radiology has not received any reports of misuse of information and/or related identity theft since the date the incident was discovered (July 9, 2023 to present). .

2. Maryland Residents Notified

One (1) Maryland resident was potentially affected by this security incident. A notification letter was mailed to the potentially impacted individual on August 14, 2023, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Although TRACT Radiology is not aware of any evidence of misuse of personal information, TRACT Radiology has extended to the potentially impacted individual an offer for free credit monitoring and identity theft protection through Sontiq. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise. TRACT Radiology has changed passwords, strengthened password requirements, and implemented stricter multi-factor authentication requirements.

4. Contact Information

TRACT Radiology remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Erica.Lloyd@LewisBrisbois.com or 601.499.8127.

Very truly yours,

Lewis Brisbois Bisgaard & Smith LLP

A handwritten signature in black ink, appearing to read "Erica J. Lloyd". The signature is fluid and cursive, with the first name "Erica" and last name "Lloyd" clearly distinguishable.

Erica J. Lloyd, Esq.

Enclosures: *Sample Notification Letter*

Radiology Consultants of Tulsa
c/o Cyberscout, a TransUnion company
PO Box 1286
Dearborn, MI 48120-9998

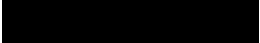
P



August 14, 2023

Via First-Class Mail

Notice of Data Incident

Dear ,

You are receiving this letter because you are a current or former patient of Radiology Consultants of Tulsa. We are writing to inform you of an incident that may have exposed your personal information. At Radiology Consultants of Tulsa, we take your privacy seriously and want to provide you with information and resources you can use to protect your information.

What Happened:

On July 9, 2023, Radiology Consultants of Tulsa experienced a network security incident that involved an unauthorized party gaining access to our network environment. Upon detecting the incident, we immediately shut off all access to the network and engaged a specialized third-party forensic incident response firm to assist with securing the network environment and investigating the extent of unauthorized activity. The Radiology Consultants of Tulsa network has been secured.

Radiology Consultants of Tulsa has no evidence that your information has been misused. However, the investigation determined that the unauthorized third party may have accessed certain personal information as a result of this incident.

What Information Was Involved:

Again, we found no evidence that your information has been misused. However, it is possible that the following personal information could have been accessed by an unauthorized third party: first name, last name, address, Social Security number, date of birth, medical information, billing information, and health insurance information.

What We Are Doing:

Data security is among our highest priorities. Upon detecting this incident we moved quickly to initiate a response, which included conducting an investigation with the assistance of third-party IT specialists and confirming the security of our network environment. We notified law enforcement. We wiped and rebuilt affected systems and have taken steps to bolster our network security. We are also reviewing and altering our policies, procedures, and network security software relating to the security of our systems and servers, as well as how we store and manage data.

000010102G0400

P

Additionally, while we have no evidence that your information has been misused in any manner, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is 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 Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/tract> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. 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. 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 encourage you to take full advantage of this service offering. Enclosed you will find additional materials regarding the resources available to you, and the steps you can take to further protect your personal information.

Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. Please call Cyberscout at 1-833-760-0277, Monday through Friday, 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays, for assistance or for any additional questions you may have.

Thank you for entrusting Incident with your healthcare needs. We value the security of the personal data that we maintain, and understand the frustration, concern, and inconvenience that this incident may have caused. We look forward to continuing to provide high quality care to you, your family, and the Tulsa community.

Sincerely,

Radiology Consultants of Tulsa

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are listed above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.



File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

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 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 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 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.

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, and <https://ag.ny.gov/>.

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, 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 is approximately 1 Rhode Island resident that may be impacted by this event.