

**Karen Bridges**  
Direct Dial: 312.642.7127  
E-mail: [kbridges@mcdonaldhopkins.com](mailto:kbridges@mcdonaldhopkins.com)

August 28, 2024

**VIA EMAIL ([Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us))**

Office of the Maryland Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202

**Re: Radiological Society of North America – Incident Notification**

To Whom It May Concern:

McDonald Hopkins PLC represents Radiological Society of North America (“RSNA”). I am writing to provide notification of an incident at RSNA that may affect the security of personal information of approximately nine (9) Maryland residents. By providing this notice, RSNA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about June 25, 2024, RSNA detected unauthorized access to its network. Upon learning of this issue, RSNA immediately secured their environment and commenced a prompt and thorough investigation. As part of their investigation, RSNA has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, on July 26, 2024, RSNA discovered that between June 20, 2024 and June 26, 2024, certain impacted files containing personal information may have been accessed and/or acquired by an unauthorized individual. The personal information contained within the impacted data included first and last name, and Social Security number.

RSNA has no evidence of financial fraud or identity theft related to this data. Nevertheless, out of an abundance of caution, RSNA wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. RSNA is providing the affected residents with notification of this incident, commencing on or about August 28, 2024. The notice will be in substantially the same form as the letter attached hereto. RSNA is also offering the affected residents whose Social Security number was potentially impacted by the incident with complimentary credit monitoring services. RSNA is advising the affected residents to always remain vigilant in reviewing financial account statements, explanation of benefits statements, and credit reports for fraudulent or irregular activity on a regular basis. RSNA is also advising the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected residents are being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

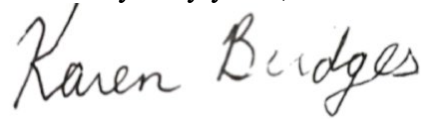
August 28, 2024

Page 2

At RSNA, protecting the privacy of personal information is a top priority. RSNA is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. RSNA continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at (312) 624-7127 or [kbridges@mcdonaldhopkins.com](mailto:kbridges@mcdonaldhopkins.com)

Very truly yours,

A handwritten signature in dark ink that reads "Karen Bridges". The signature is written in a cursive, flowing style.

Karen Bridges

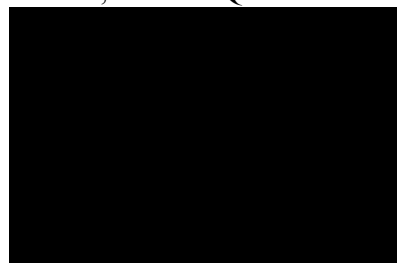
Encl.



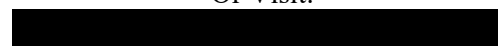
P.O. Box 989728  
West Sacramento, CA 95798-9728

Enrollment Code: [REDACTED]

To Enroll, Scan the QR Code Below:



Or Visit:



August 28, 2024

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Radiological Society of North America ("RSNA"). We are writing with important information regarding a recent data security incident that may have impacted some of your information. As such, we want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about June 25, 2024, RSNA detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the potential exposure of a limited number of 1099 forms.

What We Are Doing.

Upon learning of this issue, we immediately secured the environment and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation and manual document review, on July 26, 2024 we discovered that between June 20, 2024 and June 26, 2024, certain impacted files containing personal information may have been accessed and/or acquired by an unauthorized individual.

What Information Was Involved?

The impacted information includes your [REDACTED]

What You Can Do.

**We have no evidence that any of your information has been used for identity theft or financial fraud as a result of this incident.** Nevertheless, to protect you from potential misuse of your information, we are offering identity theft protection services through IDX, a ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: [REDACTED] months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is November 28, 2024.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

*For More Information.*

Please accept our apologies that this incident occurred. RSNA is committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. RSNA continually evaluates and modifies its practices and internal controls to enhance the security and privacy of your personal information.

**If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED]** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, [REDACTED] to [REDACTED] pm Pacific Time.

Sincerely,

**Radiological Society of North America**  
820 Jorie Blvd., Suite 200  
Oak Brook, IL 60523-2251

**– OTHER IMPORTANT INFORMATION –**

**1. Enrolling in Complimentary [REDACTED] Months of Credit Monitoring.**

- **Website and Enrollment.** Scan the QR image or go to [REDACTED] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- **Telephone.** Contact IDX at [REDACTED] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

**2. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

***Equifax***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/cen-ter.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance  
Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

**3. Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

***Equifax Security Freeze***

P.O. Box 105788  
Atlanta, GA 30348-5788  
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>  
(888) 298-0045

***Experian Security Freeze***

P.O. Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
(888) 397-3742

***TransUnion Security Freeze***

P.O. Box 160  
Woodlyn, PA 19094  
<https://www.transunion.com/credit-freeze>  
(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

#### **4. Obtain and Monitor Your Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

#### **5. Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

**Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

**New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

**Oregon Residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392.

**Washington D.C. Residents:** You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

**Rhode Island Residents:** You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a “security freeze” on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may 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. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver’s license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There were 2 Rhode Island residents impacted by this incident.