WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
spollock@wtplaw.com

7 ST. PAUL STREET
BALTIMORE, MD 21202-1636
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

January 7, 2022

Privileged and Confidential
SUBMITTED VIA THE ONLINE PORTAL ONLY:
https://appengine.egov.com/apps/me/maine/ag/reportingform
Office of the Attorney General

Re: Security Breach Notification

Dear Sir or Madam,

We are writing on behalf of our client, Medical Review Institute of America ("MRIoA") (located at 2875 South Decker Lake Drive, Salt Lake City, UT 84119) and some of its health provider and other customers, to notify you of a data security incident involving one hundred and ninety-four (194) Maine residents.[1][2]

Nature

On November 9, 2021, MRIoA discovered that it was the victim of a sophisticated cyber incident that resulted in unauthorized access to its network. At that time, MRIoA took immediate steps to stop the threat and understand the full scope of the situation. This included hiring third-party forensic experts to conduct a thorough investigation, technological remediation efforts, and contacting the FBI to seek assistance with the incident. The forensic investigation recently concluded and found that the unauthorized individual gained access to its systems via a SonicWall vulnerability on November 2, 2021, that has been removed, and MRIoA's environment has been secured.

On November 16, 2021, to the best of its ability and knowledge, MRIoA retrieved and subsequently confirmed the deletion of the obtained information. Subsequently, MRIoA began a comprehensive search of the data to determine what information was involved and the individuals the incident impacted. MRIoA recently concluded its review and determined that the incident involved personal information related to 194 Maine residents.

The personal information potentially involved (only if this information was provided to MRIoA) is demographic information (i.e., first and last name, gender, home address, phone number, email address, date of birth, and social security number); clinical information (i.e., medical history/diagnosis/treatment, dates of service, lab test results, prescription information, provider name, medical account number, or

[1] By providing this notice, MRIoA does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine's data event notification statute, or personal jurisdiction.

[2] Exhibit B includes the list of some of MRIoA's customers on whose behalf MRIoA is submitting this notification.

anything similar in your medical file and/or record); and financial information (i.e., health insurance policy and group plan number, group plan provider, claim information).

Notice and MRIoA's Response to the Event

On January 7, 2022, MRIoA will mail a written notification to the potentially affected Maine residents, pursuant to 10 Me. Rev. Stat. § 1346, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, MRIoA is providing these potentially impacted individuals the following:

- Free access to credit monitoring services for one year, through Kroll;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- 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 and law enforcement to report attempted or actual identity theft and fraud.

Further, MRIoA provided the notice to the three nationwide consumer reporting agencies, applicable government regulators, officials, and other Attorneys General (as necessary). Finally, MRIoA implemented and/or are continuing to implement additional cybersecurity safeguards to our existing robust infrastructure to better minimize the likelihood of this type of event occurring again, including:

- Constant monitoring of its systems with advanced threat hunting and detection software;
- Adding additional authentication protections when attempting to access the systems;
- New servers built from the ground up to ensure all threat remnants were removed;
- Working with external third-party cybersecurity experts to assist in their security efforts;
- Deploying a hardened and new backup environment;
- Enhancing its employee cybersecurity training; and
- Reviewing, revising, and amending its existing cybersecurity policies as necessary.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-8002 or email me at spollock@wtplaw.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

MRIoA® MEDICAL REVIEW INSTITUTE of AMERICA, LLC

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

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

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

At the Medical Review Institute of America ("MRIoA"), we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that involves your protected personal information, what we did in response, and steps you can take to protect yourself against possible misuse of the information. Please note that you are receiving this letter because <<b2b_text_1 (Covered Entity)>> provided us information to facilitate a clinical peer review of a health care service you requested or received.

What Happened

On November 9, 2021, we learned that we were the victim of a sophisticated cyber-attack. Once we found out, we quickly took steps to secure and safely restore our systems and operations. Further, we immediately engaged third-party forensic and incident response experts to conduct a thorough investigation of the incident's nature and scope and assist in the remediation efforts. We also contacted the FBI to inform them of the incident and seek guidance. On November 12, 2021, we discovered that the incident involved the unauthorized acquisition of information.

On November 16, 2021, to the best of our ability and knowledge, we retrieved and subsequently confirmed the deletion of the obtained information. Our investigation into the cause of the incident is ongoing. However, once we retrieved the information, we began determining the individuals impacted in the incident. Further, based on a comprehensive review, we discovered that your protected health information was included in the incident. ***However, as of now, we have no evidence indicating misuse of any of your information.***

What Information Was Involved

The types of protected health information potentially involved (only if this information was provided to MRIoA by the organization named above) are your demographic information (i.e., first and last name, gender, home address, phone number, email address, date of birth, and social security number); clinical information (i.e., medical history/diagnosis/treatment, dates of service, lab test results, prescription information, provider name, medical account number, or anything similar in your medical file and/or record); and financial information (i.e., health insurance policy and group plan number, group plan provider, claim information).

What We Are Doing

As explained above, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we implemented and/or are continuing to implement additional cybersecurity safeguards to our existing robust infrastructure to better minimize the likelihood of this type of event occurring again, including:

- Constant monitoring of our systems with advanced threat hunting and detection software;
- Adding additional authentication protections when attempting to access the systems;
- New servers built from the ground up to ensure all threat remnants were removed;
- Working with external third-party cybersecurity experts to assist us in our security efforts;
- Deploying a hardened and new backup environment;
- Enhancing our employee cybersecurity training; and
- Reviewing, revising, and amending our existing cybersecurity policies as necessary.

What You Can Do

The security and privacy of the information contained within our systems is a top priority for us. Therefore, while we have no evidence indicating your information was misused, we strongly recommend that you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement. In addition, please see ***"OTHER IMPORTANT INFORMATION"*** on the following pages for guidance on how to best protect your identity.

Further, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, 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 (Activation Deadline)>> 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.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. To assist you with questions regarding this incident, representatives are available for 90 days from the date of this letter, between the hours of 8:00 am to 5:30 pm Central time (excluding major U.S. holidays), Monday through Friday. Please call the helpline 1-855-618-3157 and supply the call center representative with your unique code listed above. To extend these services, enrollment in the monitoring services described above is required.

Sincerely yours,

Ron Sullivan, President/CEO

KROLL

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 will 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

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.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	**(888) 397-3742**	**(800) 680-7289**
P.O. Box 740256	P.O. Box 2104	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below).

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze & Fraud Victim Assistance Dept.**
P.O. Box 105788	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	https://www.transunion.com/credit-freeze

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. 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 on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov. **Iowa residents** may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: *Office of the Attorney General of Iowa,* Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319. **Maryland residents** may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **Massachusetts residents**: State law advises you that you have the right to obtain a police report. Further, you have the right to obtain a security freeze on your credit report free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. To request a security freeze be placed on your credit report, please be prepared to provide any or all of the following: your full name, social security number, address(es), date of birth, a copy of a government issued identification card, a copy of a utility bill, bank or insurance information, or anything else the credit reporting agency needs to place the security freeze. Further information regarding credit freezes, including the contact information for the credit reporting agencies, may be found above in section titled "Security Freeze (also known as a Credit Freeze)." **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **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. **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: New York Attorney General's Office Bureau of Internet and Technology, (212) 416-8433, https://ag.ny.gov/internet/resource-center and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, https://www.dos.ny.gov/consumerprotection. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at www.ncdoj.gov, or by contacting the Attorney General by calling 877-5-NO-SCAM (Toll-free within North Carolina) or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office, Consumer Protection Division,* 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. **West Virginia residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.

EXHIBIT B

- Albertsons Companies
- AllWays Health Partners
- Ambetter from Home State Health
- Ambetter From Superior Health Plan
- Ambetter of North Carolina
- Blue Cross & Blue Shield of Rhode Island
- Blue Cross and Blue Shield of Minnesota
- Blue Cross Blue Shield of Illinois
- Blue Cross Blue Shield of New Jersey
- Blue Cross Blue Shield of Texas
- Cambia Health Solutions
- Capital Blue Cross
- CARY MEDICAL CENTER
- Florida Blue
- General Dynamics
- Genex Services, LLC
- Government Employees Health Association, Inc.
- Health New England
- Horizon
- Horizon Blue Cross Blue Shield of New Jersey
- Magellan Rx Medicare Basic PDP
- MAINEGENERAL HEALTH
- National Elevator Industry Health Benefit Plan
- NORTH AMERICA ADMINISTRATORS
- OptumRx
- State of Maine Department of Administrative and Financial Services, Office of Employee Health and Wellness
- SULLIVAN TIRE
- The Associates' Health and Welfare Plan
- Twin Rivers Paper Company
- University of Arkansas Medical Benefit Plan
- WellCare