

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

SUBMITTED ONLY VIA THE ONLINE PORTAL

<https://appengine.egov.com/apps/me/maine/ag/reportingform>

Office of the Attorney General

November 23, 2021

Re: Security Breach Notification

To Whom It May Concern:

We are writing on behalf of our client, TriValley Primary Care (“TriValley”) (located at 519 S. Fifth Street, Suite 130, Perkasi, PA 18944-1042), to notify you of a data security incident involving ten (10) Maine residents.¹ TriValley is a medical organization focusing on primary care throughout Pennsylvania.

Nature

On October 11, 2021, TriValley discovered that it was the victim of a cyberattack that impacted its systems and servers which contained protected health and personal information of some TriValley patients. After discovering the incident, TriValley quickly took steps to secure and safely restore its systems and operations. TriValley engaged our firm and third-party forensic experts to assist in the remediation efforts and conduct a thorough investigation of the incident's nature and scope. TriValley also contacted the FBI to seek assistance and guidance as one of the many health care providers confronting the impacts of the evolving cyber threat landscape.

TriValley concluded its investigation on November 4, 2021, and, as of now, TriValley has no evidence indicating any misuse of patient information. TriValley determined that the unauthorized individual accessed our systems and may have obtained some information. The forensic analysis could not definitively determine when the unauthorized individual initially got into the systems or the specific records and data that were accessed or obtained. As such, TriValley conducted a comprehensive review of a significant amount of stored data to determine the types of protected information that was potentially exposed and identify individuals potentially impacted by the incident. TriValley concluded its initial review and determined that the incident potentially involved the information of ten (10) Maine residents. On November 22, 2021, TriValley located the most recent contact information for these individuals.

The types of information potentially involved (only if the affected party provided us this information) are 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 their medical file and or record); and financial information (i.e., health insurance policy and group plan number, group plan provider, claim information).

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

Notice and TriValley's Response to the Event

On November 24, 2021, TriValley will mail a written notification to the potentially affected Maine residents, pursuant to 10 M.R.S.A. §§1346-1350-B, in a substantially similar form as the enclosed letter (attached as Exhibit A). Additionally, TriValley is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for one year through Sontiq;
- 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, TriValley notified the three major credit reporting agencies and applicable government regulators, officials, and Attorneys General (as necessary). Finally, TriValley is working to implement additional safeguards to its existing cybersecurity infrastructure including enforcing MFA enterprise wide and utilizing EDR, enhancing employee cybersecurity training, and working to improve its cybersecurity policies, procedures and protocols to help minimize the likelihood of this type of incident occurring again.

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



Corporate Office
519 S. Fifth Street, Suite 130
Perkasie, PA 18944-1042
[Call Center Number]

November 24, 2021

<First Name> <Last Name>
<Street>
<City>, <State> <Zip>

Re: Notice of Data Breach

Dear <First Name> <Last Name>,

At TriValley Primary Care, 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 may involve your personal information. This notice describes what we did in response, and steps you can take to protect yourself against possible misuse of your personal information.

What Happened

On October 11, 2021, we discovered a ransomware incident that impacted our networks and servers.

After discovering the incident, we quickly took steps to secure and safely restore our systems and operations. Further, we engaged outside counsel and third-party forensic experts to assist in the remediation efforts and conduct a thorough investigation of the incident's nature and scope. We also contacted the FBI to seek assistance and guidance, as one of the many health care providers confronting the impacts of the evolving cyber threat landscape.

We concluded our investigation on November 4, 2021, and, as of now, **we have no evidence indicating any misuse of your information.** We determined that the unauthorized individual accessed our systems and may have obtained some information. The forensic analysis could not definitively determine when the unauthorized individual initially got into the systems or the specific records and data that were accessed or obtained. As such, since we are unable to confirm that your protected health information was not accessed and or obtained, out of an abundance of caution we wanted to notify you of the incident and provide you with information on steps you can take to help protect your information.

What Information Was Involved

The types of information potentially involved (only if you provided us this information) 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).

However, to date, we have no evidence indicating any misuse of this information in connection with this incident.

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us.

In response to this incident, we are implementing additional safeguards to our existing cybersecurity infrastructure and enhancing our employee cybersecurity training. Further, we are working with cybersecurity experts to improve our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

What You Can Do

As stated above, while we have no evidence indicating your information was misused, we strongly recommend 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 steps you can take to help protect your information.

Also, we are providing you with access to Single Bureau Credit Monitoring * services at no charge. These services provide you with alerts for twelve (12) 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to **www.xxx.com** and follow the instructions provided.

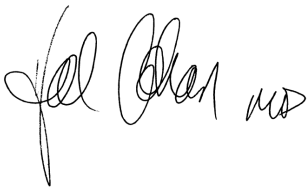
When prompted please provide the following unique code to receive services: **<access code>**

In order for you to receive the monitoring services described above, you **must enroll within 90 days** from the date of this letter.

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. If you have any additional questions, please contact the external, dedicated call center we set up at [number] from 8:00 am to 8:00 pm Eastern time, Monday through Friday (except holidays). Representatives are available for 90 days.

Sincerely yours,

A handwritten signature in black ink that reads "Hal Cohan MD". The signature is written in a cursive style with a large initial "H" and "C".

Hal Cohan, MD, Chairman, TriValley Primary Care

* Services marked with an “*” require 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.

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.

<p>Equifax (888) 766-0008 P.O. Box 740256 Atlanta, GA 30374 www.equifax.com</p>	<p>Experian (888) 397-3742 P.O. Box 2104 Allen, TX 75013 www.experian.com</p>	<p>TransUnion (800) 680-7289 P.O. Box 1000 Chester, PA 19016 www.transunion.com</p>
--	---	---

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 above).

<p>Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/</p>	<p>Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze</p>	<p>TransUnion Security Freeze & Fraud Victim Assistance Dept. P.O. Box 6790 Fullerton, CA 92834 https://www.transunion.com/credit-freeze</p>
--	--	---

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/pdf0009_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 20001, 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. You also will not be charged for seeking a security freeze, as described above in this document. **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 <https://ncdoj.gov/protecting-consumers/identity-theft/>, or by contacting the Attorney General by calling 1-877-566-7226 or emailing or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office* 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.