NORTON ROSE FULBRIGHT

April 2, 2021

Norton Rose Fulbright US LLP
799 9th Street NW
Suite 1000
Washington, DC 20001-4501
United States

Direct line +1 202 662 4691
chris.cwalina@nortonrosefulbright.com

Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

Via: Certified Mail

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Data Security Incident

Dear Sir or Madam:

I am writing on behalf of my client, Bricker & Eckler LLP ("Bricker"), to notify your office that Bricker was the target of a ransomware attack that involved the personal information of 15 New Hampshire residents.

Bricker, a full-service law firm with offices throughout Ohio and clients across the country, services companies and organizations across a variety of industries, and in the course of its work on behalf of clients is at times provided access to personal information as a part of the client engagement. Bricker receives and utilizes this data in its representation of, and to provide legal counsel to, its clients.

On January 31, 2021, Bricker discovered it was targeted by a ransomware attack in which an unauthorized actor deployed Sodinokibi ransomware across Bricker's systems. Bricker immediately launched an investigation and engaged cybersecurity and forensic firms to determine the nature and scope of the incident. Bricker also notified the Federal Bureau of Investigation.

Bricker's investigation determined that an unauthorized party gained access to certain Bricker internal systems at various times between approximately January 14, 2021 and January 31, 2021. Findings from the investigation indicate that the unauthorized party obtained some data from certain Bricker systems during this period. Bricker was able retrieve the data involved from the unauthorized party and has taken steps to delete the data. At this time, Bricker has no reason to believe this data was further copied or retained by the unauthorized party. On March 10, 2021, Bricker completed its review of the data and began notifying clients of any client-related personal information included in these files.

The Bricker clients set forth in the attached ***Appendix A***, have asked that Bricker provide notice to your office on its behalf. The review determined that the files contained the following types of affected individuals' personal information: name, address, date of birth, health-related information, education-related information, Social Security numbers, and driver's license numbers.

Bricker is not aware of any fraud or misuse of any personal information as a result of this incident. Bricker does not believe personal information was targeted by the unauthorized party for identity

theft purposes, but rather, such information happened to be included in documents taken by the unauthorized party as part of the ransomware attack to extort the company.

On or around April 6, 2021, Bricker will begin sending notification letters via First Class Mail to the affected individuals whose personal information was involved on its own behalf, and on behalf of the Bricker clients set forth in Appendix A. A copy of the notice letter is attached. Bricker is offering 12 months of complimentary credit monitoring and fraud protection services to these individuals. Bricker is also providing a toll-free hotline for the individuals to call with any questions regarding the incident.

To help prevent a similar type of incident from occurring in the future, Bricker implemented additional security protocols designed to enhance the security of its network, internal systems and applications. Bricker also continues to evaluate additional steps that may be taken to further increase its defenses going forward.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Very truly yours,

Chris Cwalina

CGC/

Enclosure

Appendix A

1	TriHealth, Inc. Company Address: 625 Eden Park Drive, Cincinnati, OH 45202 Point of Contact Name: Candice Kramer Point of Contact Email: Candice_Kramer@TriHealth.com Point of Contact Phone Number: 513-569-5507

Bricker&Eckler
ATTORNEYS AT LAW

April 6, 2021

[**FIRST NAME**] [**LAST NAME**]

[**ADDRESS**]

Re: Notice of Data Security Incident

Dear [**FIRST NAME**]:

Bricker & Eckler LLP ("Bricker"), a full-service law firm with offices throughout Ohio and clients across the country, was recently the target of a ransomware attack. Bricker services companies and organizations across a variety of industries, and in the course of its work on behalf of clients is at times provided access to personal information as a part of the client engagement. Bricker receives and utilizes this data solely in its representation of and to provide legal counsel to its clients.

Bricker is writing to inform you that the incident may have involved some of your personal information. Bricker was in possession of that information due to its work on behalf of [**BRICKER CLIENT**]. This notice explains the incident, steps Bricker has taken in response, and additional information on steps you may take to help protect your information.

What Happened?

On January 31, 2021, Bricker learned that it was the target of a ransomware attack. Upon learning of the incident, Bricker immediately took measures to contain the incident, launched an investigation, and third-party cybersecurity forensic experts were engaged to assist. Bricker also notified federal law enforcement.

The investigation determined that an unauthorized party gained access to certain Bricker internal systems at various times between approximately January 14, 2021 and January 31, 2021. Findings from the investigation indicate that the party obtained some data from certain Bricker systems during this period. Bricker was able retrieve the data involved from the unauthorized party and has taken steps to delete the data. At this time, Bricker has no reason to believe this data was further copied or retained by the unauthorized party. Bricker conducted a thorough review of the data to identify individuals whose personal information may have been involved.

What Information Was Involved?

The review determined that the data involved contained some of your personal information, which may have included your name, address, **[VARIABLE DATA FIELD].**

What We Are Doing

To help prevent a similar type of incident from occurring in the future, Bricker implemented additional security protocols designed to enhance the security of Bricker's network, internal systems and applications. Bricker will also continue to evaluate additional steps that may be taken to further increase Bricker's defenses going forward. In addition, Bricker is continuing to support federal law enforcement's investigation.

What You Can Do

At this time, there is no evidence that your personal information has been misused, but Bricker wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. As a precaution, Bricker is offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **[DATE]** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **[URL]**
- Provide your activation code: **[XXXXX]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **[EXPERIAN CONTACT NUMBER]** by **[ENROLLMENT END DATE]**. Be prepared to provide engagement number **[XXXX]** as proof of eligibility for the identity restoration services by Experian.

For More Information

The security of your personal information is important to Bricker and Bricker sincerely regrets that this incident occurred. For more information, or if you have any questions or need additional information, please call **[EXTERNAL CALL CENTER NUMBER]**, Monday through Friday, between **[XX:XX]** a.m and **[X:XX]** p.m. Eastern Time.

Sincerely,

Bricker & Eckler LLP

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring**: Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration**: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance****: Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there, was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (855) 414-6050. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:
You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

For New Mexico residents: 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 may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report.
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.