DLA Piper LLP (US)
One Liberty Place
1650 Market Street
Suite 5000
Philadelphia, Pennsylvania
19103-7300

Ron Plesco
+1 215.656.2453
Ron.Plesco@us.dlapiper.com

October 14, 2022

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Security Incident Notification

Dear Attorney General Frosh:

I am writing on behalf of Three Rivers Provider Network ("TRPN") pursuant to Md. Code Ann., Com. Law § 14-3504, regarding an incident involving three (3) Maryland residents.

On June 3, 2022, TRPN identified access to one (1) employee email account by an unauthorized party (the "Incident"). The internal security team immediately took steps to secure the impacted account, including changing the password to the account and removing the suspicious device from multi-factor authentication. Upon discovery, TRPN promptly launched a comprehensive investigation with the assistance of cybersecurity experts to undertake a full forensic analysis of the Incident.

TRPN's in-depth investigation of the Incident determined that the unauthorized user gained access to the compromised account on June 1, 2022, and the last unauthorized activity in the account occurred on June 3, 2022. With the assistance of cybersecurity experts, TRPN worked diligently to analyze impacted data potentially accessed by the unauthorized user to identify potentially impacted personal information. On August 17, 2022, the results of the investigation revealed that personal information was impacted. TRPN later determined that information relating affected Maryland residents was potentially impacted. Please also note that our review of the compromised account to identify potentially impacted personal information remains ongoing.

The information affected varies by individual but includes one or more of the following types of personal information: names, addresses, emails addresses, dates of birth, social security numbers, passport numbers, driver's license numbers, health insurance numbers, and health information. It does not include credit card numbers or sensitive financial information.

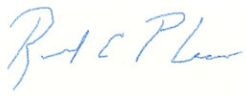
TRPN has implemented additional security measures to prevent this activity from occurring in the future including, but not limited to, creating new conditional access rules to prevent access from unauthorized IP addresses; implementing new monitoring and alert rules to detect access from first time IP addresses and improbable travel scenarios; and updating MFA protocols. Please note that TRPN has reviewed their Microsoft Office 365 email environment for indications of unauthorized access to any other TRPN email accounts. The investigation did not identify any additional TRPN email accounts with indications of unauthorized access. TRPN continues to monitor the Internet for potential misuses of Maryland residents' data, and there is no indication to suggest the impacted data is being misused.

On October 15, 2022, TRPN will begin mailing notice to the affected Maryland residents, offering a 24-month subscription for credit monitoring and identity protection through Equifax Complete Premier Credit Monitoring and Identity Theft protection. Affected residents may enroll in the services at no cost by using a promotional code and instructions provided to them in the notification letter.

A sample notification letter is enclosed.

Should you have any questions regarding this matter or if we can be of any further assistance to the Maryland residents affected by this Incident, please contact me at Ron.Plesco@us.dlapiper.com.

Respectfully submitted,



Ron Plesco
Partner, DLA Piper LLP

Enclosure: Sample Notification Letter

THREE RIVERS PROVIDER NETWORK

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 15, 2022

i4752-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L02 GENERAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: **NOTICE OF DATA BREACH**

Dear Sample A. Sample:

On behalf of Three Rivers Provider Network ("TRPN"), we write to inform you of an incident that may have involved personal information about you. We deeply regret that this incident occurred and take seriously the security of personal information.

WHAT HAPPENED? On June 3, 2022, TRPN identified unauthorized access to one (1) employee email account by an unauthorized party. We immediately initiated an investigation and secured the compromised account. On August 17, 2022, we discovered that your personal information may have been accessed by the unauthorized party.

WHAT INFORMATION WAS INVOLVED? Personal information that may be affected includes your name, address, date of birth, social security number, treatment or diagnosis information, prescription information, provider name, MRN or patient ID number, Medicare or Medicaid number, health insurance information, health insurance policy number, or treatment cost information.

WHAT WE ARE DOING. We have thoroughly investigated this incident and taken additional steps to secure our systems. Please know that protecting your personal information is something that we take very seriously, and we value your trust in doing business with us. We apologize for both this unfortunate incident and any inconvenience it may cause you. We have taken steps to address the incident and ensure that this does not occur in the future. We are providing notice and offering credit monitoring services to individuals based on the personal information that was potentially impacted.

WHAT YOU CAN DO. We are confident that no financial information, such as financial account information or credit card numbers was involved in this incident. You should be on guard for schemes, known as phishing attacks, where malicious actors may pretend to represent TRPN or reference this incident. If you have questions, please contact us at the number described below. To help protect your identity, we are offering **complimentary** credit monitoring services as described below. This helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft.

OTHER IMPORTANT INFORMATION. The Federal Trade Commission (FTC) recommends that you remain vigilant by checking your credit reports periodically. Checking your credit reports can help you spot problems and address them quickly. You can also order free copies of your annual reports through www.annualcreditreport.com. You should monitor your financial accounts for any suspicious activity. For more information about steps you can take to reduce the likelihood of identity theft or fraud, call 1-877-IDTHEFT or 1-877-438-4338, visit the FTC's website at www.ftc.gov/bcp/edu/microsites/idtheft/ or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. However, if you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state's attorney general, or the FTC.

Credit Monitoring Instructions

We have arranged for you to receive free credit monitoring to help you protect your identity and credit information. (See enclosed instructions.) If you choose to enroll, you will receive communications detailing any key changes to your credit reports. To enroll in this service, please contact Equifax by calling the phone number listed below. If you have internet access, you may also enroll by visiting the website listed below. To enroll, you will also need the Activation Code provided below. Your coverage will last for 24 months from the date of enrollment.

Enrollment URL:	**www.equifax.com/activate**
Your Activation Code:	**ABCDEFGHI**
Enrollment Deadline:	**January 31, 2023**

Contact Information for Consumer Reporting Agencies and Information on Credit Report Fraud Alerts

You may also choose to place a fraud alert on your credit file, which is free of charge to you and can be done with any ***one*** of the companies listed below (i.e., if you place a fraud alert with one company, they will automatically notify the others). A fraud alert tells creditors to contact you ***before*** they open any new accounts or change your existing accounts.

	Experian	**Equifax**	**TransUnion**
Phone	1-888-397-3742	1-800-525-6285 or 1-888-766-0008	1-800-680-7289
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	www.experian.com/fraud/center.html	www.equifax.com/personal/credit-report-services	fraud.transunion.com/fa/fraudAlert/landingPage.jsp

Information on Security Freezes

In addition to a fraud alert, you may place a security freeze on your credit file. A security freeze ***will block*** a credit bureau from releasing information from your credit report ***without your prior written authorization***. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. There is no cost to place, lift or remove a security freeze.

To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online. Please provide the information requested, which varies by consumer reporting agency, but typically includes: full name, address, Social Security number, date of birth, proof of identity and proof of address.

	Experian	**Equifax**	**TransUnion**
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	www.experian.com/freeze/center.html	www.equifax.com/personal/credit-report-services	www.transunion.com/test/new-freeze

You may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes.

FOR MORE INFORMATION. If you have questions about the data breach, please call 855-904-2303 (Monday - Friday 9am-5pm EST).We sincerely regret that this incident occurred.

Sincerely,

Scott Smith

State-Specific Information

If you are a resident of the following states, the following information applies to you.

For residents of Maryland, New York, North Carolina, Rhode Island, the District of Colombia: For information on how to avoid identity theft or to contact your state's attorney general, please use the below information.

Maryland Attorney General	**North Carolina Attorney General**	**Rhode Island Attorney General**
1-888-743-0023 www.oag.state.md.us Attorney General of Maryland 200 St. Paul Place Baltimore, MD 21202	1-877-566-7226 www.ncdoj.gov Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001	1-401-274-4400 www.riag.ri.gov Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903
District of Colombia Attorney General	**New York Attorney General**	
1-202-727-3400 www.oag.dc.gov Office of the Attorney General for the District of Columbia 441 4th St. NW Washington, DC 20001	1-800-771-7755 www.ag.ny.gov Office of the Attorney General The Capitol Albany, NY 12224-0341	

For residents of New Mexico: You have rights under the federal Fair Credit Reporting Act (FCRA). These include: the right to access information in your consumer file at a consumer reporting agency; to dispute incomplete or inaccurate information in your consumer file at a consumer reporting agency; to have consumer reporting agencies correct or delete inaccurate information in your consumer file; the right to block information in your consumer file that is the result of identity theft; and the right to have a fraud alert placed on your consumer file (as described above). For more information, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

For residents of Rhode Island: Under Rhode Island law, you have the right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

EQUIFAX®

Sample A. Sample
Enter your Activation Code: **ABCDEFGHI**
Enrollment Deadline: **January 31, 2023**

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **ABCDEFGHI** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1] The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

[2] Credit monitoring from Experian and TransUnion will take several days to begin.

[3] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[4] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[5] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

[6] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

DLA Piper LLP (US)
One Liberty Place
1650 Market Street
Suite 5000
Philadelphia, Pennsylvania
19103-7300

Ron Plesco
(215) 656-2453
Ron.Plesco@us.dlapiper.com

November 9, 2022

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Security Incident Notification

Dear Attorney General Frosh:

I am writing on behalf of Three Rivers Provider Network ("TRPN") pursuant to Md. Code Ann., Com. Law § 14-3504, regarding an incident TRPN first reported on behalf of its clients on October 14, 2022.

On June 3, 2022, TRPN identified access to one (1) employee email account by an unauthorized party (the "Incident"). The internal security team immediately took steps to secure the impacted account, including changing the password to the account and removing the suspicious device from multi-factor authentication. Upon discovery, TRPN promptly launched a comprehensive investigation with the assistance of cybersecurity experts to undertake a full forensic analysis of the Incident.

TRPN's in-depth investigation of the Incident determined that the unauthorized user gained access to the compromised account on June 2, 2022, and the last unauthorized activity in the account occurred on June 3, 2022. With the assistance of cybersecurity experts, TRPN worked diligently to analyze impacted data potentially accessed by the unauthorized user to identify potentially impacted personal information. On August 17, 2022, the results of the investigation revealed that personal information of certain TRPN clients was impacted. TRPN later determined three (3) Maryland residents were potentially impacted. TRPN mailed notifications on October 15, 2022.

On October 8, 2022, our investigation determined an additional eleven (11) Maryland individuals of TRPN clients were potentially impacted. TRPN then worked with their clients to confirm that notices should be mailed on their behalf.

The information affected varies by individual but includes one or more of the following types of personal information: names, addresses, emails addresses, dates of birth, social security numbers, passport numbers, driver's license numbers, health insurance numbers, and health information. It does not include credit card numbers or sensitive financial information. The notification letter sent to impacted Maryland residents will identify the specific data elements impacted for each individual receiving notice.

TRPN has implemented additional security measures to prevent this activity from occurring in the future including, but not limited to, creating new conditional access rules to prevent access from unauthorized IP addresses; implementing new monitoring and alert rules to detect access from first time IP addresses and improbable travel scenarios; and updating MFA protocols. Please note that TRPN has reviewed their Microsoft Office 365 email environment for indications of unauthorized access to any other TRPN email accounts. The investigation did not

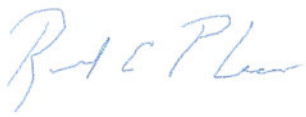
identify any additional TRPN email accounts with indications of unauthorized access. TRPN continues to monitor the Internet for potential misuses of Maryland residents' data, and there is no indication to suggest the impacted data is being misused.

On November 5, 2022, TRPN mailed notifications to the additional affected Maryland residents, offering a 24-month subscription for credit monitoring and identity protection through Equifax Complete Premier Credit Monitoring and Identity Theft protection. Affected residents may enroll in the services at no cost by using a promotional code and instructions provided to them in the notification letter.

A sample notification letter is enclosed.

Should you have any questions regarding this matter or if we can be of any further assistance to the Maryland residents affected by this Incident, please contact me at Ron.Plesco@us.dlapiper.com.

Respectfully submitted,



Ron Plesco
Partner
DLA Piper LLP

Enclosure: Sample Notification Letter