



Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

WWW.HSELAW.COM

May 23, 2022

CONFIDENTIAL

VIA EMAIL

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

Re: Data Incident Notification

To Whom It May Concern:

Harter Secrest & Emery LLP represents Trillium Health, Inc., a community health center located at 259 Monroe Avenue, Rochester, New York 14607. On or about April 12, 2022, Trillium discovered suspicious activity relating to a single Trillium user's electronic mailbox. Once it became aware of this activity, an investigation was undertaken that ultimately confirmed that an unknown and unauthorized actor had potential access to the mailbox for a short period of time, between April 8, 2022 and April 12, 2022, and that the unauthorized actor may have acquired some or all of the mailbox contents. A review of the affected mailbox was then undertaken and the personal information of a limited number of individuals was located within its contents, including the name, date of birth and social security number of a single resident of Maryland.

Once the incident was discovered, Trillium immediately took steps to address it. Working with its internal IT department and an outside forensics firm, Trillium reacted swiftly to the incident and has no reason to believe that its systems are otherwise currently at risk. In order to prevent any further unauthorized access, Trillium is taking several precautionary measures, such as changing passwords and modifying internal e-mail settings and controls, including through the implementation of multi-factor authentication.

Page 2

The affected Maryland resident will receive written notice by way of letter dated May 23, 2022, which will be mailed to the address of the affected individual. A template of the notice being sent is enclosed with this letter.

Trillium is offering the affected Maryland resident 24 months of Experian IdentityWorks fraud detection and credit monitoring services at no cost to the resident. A description of this product is set forth in the attached notification letter.

Should you have questions, please contact me using the below information. Thank you.

Very truly yours,

Harter Secrest & Emery LLP



Daniel J. Altieri
DIRECT DIAL: 716.844.3741
EMAIL: DALTIERI@HSELAW.COM

Enc.



[Date]

[First Name] [Last Name]

[Address]

[City], [State] [Zip]

Dear [First Name]:

We are writing to inform you that Trillium Health was recently a victim of a phishing scheme designed to try to steal funds from Trillium that may have also resulted in access to some of your personal information. We take the protection and proper use of your information seriously and are providing you with an offer of complimentary credit monitoring and related services through Experian. Details regarding the incident follow below.

WHAT HAPPENED

On or about April 12, 2022, we discovered suspicious activity relating to a single Trillium user's electronic mailbox. Once we became aware of this activity, an investigation by our legal team and our cyber security firm was undertaken that ultimately confirmed that an unknown and unauthorized bad actor had potential access to the mailbox for a short period of time, between April 8, 2022 and April 12, 2022, and that the unauthorized actor may have acquired some or all of the mailbox contents. A review of the affected mailbox was then undertaken and the personal information of a limited number of individuals was located within its contents. We are writing because we discovered that your name, date of birth and social security number could have been affected.

Although we believe the intent of the unauthorized actor was to attempt to steal funds from Trillium, we are providing you with this information so that you are aware and can take steps to further protect your information as you deem appropriate.

WHAT WE ARE DOING

In order to protect against any further unauthorized access to electronic mailboxes, we are taking several precautionary measures, such as changing passwords and modifying internal e-mail settings and controls (including through multi-factor log-on requirements).

In the meantime, you may wish to take some or all of the below actions to help reduce your risk of identity theft:

- Remain vigilant, especially over the next 12 months, and review your bank accounts, credit card bills and free credit reports for unauthorized activity. Promptly report any suspected identity theft to your local law enforcement agency, the U.S. Federal Trade Commission, your State Attorney General, your financial institution, and to the Fraud Alert phone line of a consumer reporting agency. You can obtain information about fraud alerts and security freezes by contacting the three national reporting agencies below:
 - o **Equifax**, P.O. Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285;
 - o **Experian**, P.O. Box 4500, Allen, TX 75013, www.experian.com, 1-888-397-3742; and
 - o **TransUnion**, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016, www.transunion.com, 1-800-680-7289.
- Periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted.
- Place a fraud alert on your credit file by contacting any of the three credit reporting agencies listed above. A fraud alert temporarily, for a period of 90 days, requires potential creditors to take additional steps to verify your identity before issuing credit in your name.
- Place a security freeze on your consumer report. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, a security freeze may delay your ability to obtain credit. Please contact one of the three credit reporting agencies listed above for further information.
- Request and carefully review your free annual consumer credit report by visiting www.annualcreditreport.com or by calling 1-877-322-8228.

You can also contact the Federal Trade Commission to obtain information about preventing identity theft and, specifically, setting up fraud alerts and security freezes. The contact information for the Federal Trade Commission is as follows: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.ftc.gov, 1-877-382-4357.

For more information about how to prevent identity theft, you can also contact the Maryland Attorney General's Office: Maryland Attorney General; 1-888-743-0023 (Baltimore Office); 200 St. Paul Place, Baltimore, MD 21202; <http://www.marylandattorneygeneral.gov/>.

OTHER IMPORTANT INFORMATION

As a result of this incident, and to help protect your identity, we would like to offer you a complimentary 24-month 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: [] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: []
- Provide your activation code: []

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 [] by []. Be prepared to provide engagement number [] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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.
- Internet Surveillance: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- 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 []. 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 24 months 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.

FOR MORE INFORMATION

If you have questions, please contact me at (585) 545-7218. Additionally, our mailing address is 259 Monroe Avenue, Rochester, New York, 14607.

Thank you.

Sincerely,

A handwritten signature in blue ink, appearing to read "Greg Ewing", with a large, stylized loop at the end.

Greg Ewing
Chief Compliance Officer