VAIL HEALTH

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[Name]
[Address]

[Date], 2022

Dear [Name]:

On behalf of Vail Health Services, I am writing to inform you that we recently suffered a security incident affecting limited amounts of protected health information for some of our patients. After determining that a phishing attack targeted some of our employees, we promptly investigated and determined on July 14, 2022, that a third party potentially viewed information contained in certain email accounts between mid-January and mid-February. Vail Health is providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED
An unauthorized third party gained access to a limited number of Vail Health's email accounts. Once we discovered the incident, we immediately engaged third-party experts to help us investigate and respond to the incident. After identifying the affected email accounts, we engaged a data review firm to comb through the data in those accounts to identify what information they contained. That process takes some time. We ultimately received the review firm's results on July 14, 2022. Since then, we have been assessing who to notify and locating correct contact information for those involved so that we can provide them notice.

WHAT INFORMATION WAS INVOLVED
This incident exposed some of our patients' protected health information. The affected data may include information such as your name, address, date of birth, and insurance details as well as limited portions of your medical/treatment history. Based on our investigation, the third party potentially viewed the information in the files. But we have no reason to suspect the information was or will be misused.

WHAT WE ARE DOING
We worked with third-party experts to investigate and respond to the incident. And we are further securing our systems to protect your information. While our emails were already protected by passwords, we have added an additional layer of security to further lockdown access to our employees' email accounts.

WHAT YOU CAN DO
While the information that was affected is not the type that generally can lead to identity theft or fraud, we nonetheless encourage you to remain vigilant for such activity. Enclosed with this letter you will find additional steps you can take to protect yourself.

FOR MORE INFORMATION
Our patients and their information are important to us. Should you have any questions, you can contact us at (866) 985-2702, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Lisa Herota, RHIA, CHC, CHPS, CCS
Senior Director, Compliance & Privacy\Compliance & Privacy Officer

VAIL-ADT-NCM

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – While the information that was affected is not the type that generally can lead to identity theft or fraud, we nonetheless encourage you to remain vigilant for such activity by reviewing your account statements and free credit reports.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.

- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.

- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

VAIL HEALTH

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[Name]
[Address]

[Date], 2022

Dear [Name]:

On behalf of Vail Health Services, I am writing to inform you that we recently suffered a security incident affecting limited amounts of protected health information for some of our patients. After determining that a phishing attack targeted some of our employees, we promptly investigated and determined on July 14, 2022, that a third party potentially viewed information contained in certain email accounts between mid-January and mid-February. Vail Health is providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED
An unauthorized third party gained access to a limited number of Vail Health's email accounts. Once we discovered the incident, we immediately engaged third-party experts to help us investigate and respond to the incident. After identifying the affected email accounts, we engaged a data review firm to comb through the data in those accounts to identify what information they contained. That process takes some time. We ultimately received the review firm's results on July 14, 2022. Since then, we have been assessing who to notify and locating correct contact information for those involved so that we can provide them notice.

WHAT INFORMATION WAS INVOLVED
This incident exposed some of our patients' protected health information. The affected data may include information such as your name, address, date of birth, driver's license, Social Security number, and insurance details as well as limited portions of your medical/treatment history. Based on our investigation, the third party potentially viewed the information in the files. But we have no reason to suspect the information was or will be misused.

WHAT WE ARE DOING
We worked with third-party experts to investigate and respond to the incident. And we are further securing our systems to protect your information. While our emails were already protected by passwords, we have added an additional layer of security to further lockdown access to our employees' email accounts. To help protect you from fraud or identity theft, we are offering a complimentary two-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. More information can be found on the following page.

WHAT YOU CAN DO
We encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for steps you can take to protect yourself against fraud and identity theft, including activating your complimentary credit monitoring.

FOR MORE INFORMATION
Our patients and their information are important to us. Should you have any questions, you can contact us at (866) 985-2702, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Lisa Herota, RHIA, CHC, CHPS, CCS
Senior Director, Compliance & Privacy\Compliance & Privacy Officer

VAIL-ADT-CDM

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary two-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you enroll by: [redacted] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your activation code: [redacted]

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-288-8057 by [redacted], and provide them engagement number [redacted].

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/DataBreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.