Morgan Lewis

Gregory T. Parks
Partner
215.963.5170
gregory.parks@morganlewis.com

January 18, 2022

VIA US MAIL

State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Notice of Data Security Incident of Kronos as Vendor to Vail Health*

Dear Office of the Attorney General:

This Firm represents Vail Health Services ("Vail Health") and we are writing to notify you regarding the nature and circumstances of a recent data security incident involving Kronos, one of Vail Health's vendors. As you may know, Kronos has announced that it experienced a ransomware attack on its systems. Despite best efforts, Vail Health has been unable to determine whether the Kronos event has affected personal information of current and former employees of Vail Health. Vail Health is therefore providing notice to current and former employees and your office out of an abundance of caution.

On or about December 13, 2021, it came to Vail Health's attention that on December 11, 2021, Kronos, an outside timekeeping and payroll software vendor used by Vail Health, experienced a ransomware attack on systems that contained information of current and former employees of Vail Health. We know that incidents like this can sometimes involve unauthorized access to or exfiltration of personal information. Vail Health has no reason to believe that personal information of its employees has been accessed or used inappropriately at this time, but out of an abundance of caution, we are sending this notice to you.

After investigation, Vail Health has determined that information on Kronos' systems at the time of the ransomware incident may have included names, addresses, dates of birth, social security numbers, salaries, bank account information, and W-2 and W-4 information. It also may have included information of employees' dependents and beneficiaries, including names, date of birth and social security numbers.

At this time, Vail Health has no evidence that the personal information of its current and former employees has been used inappropriately. To date, Kronos has not confirmed one way or the other whether any such information was compromised. Nevertheless, Vail Health sent notifications by mail to the affected individuals to explain what happened, what information was involved, what Vail Health has done, and how affected individuals can contact Vail Health with questions. Vail Health is also making an offer of one year of credit monitoring to the affected individuals. Vail

Health's contracts with Kronos require Kronos to keep Vail Health's employee information confidential and to have security procedures in place to minimize data security incidents, and Vail Health will continue to take steps to ensure that data held by Kronos on Vail Health's behalf is adequately secured.

Further information about what Vail Health has done and is recommending to the individuals in question can be found in the enclosed notification that Vail Health sent to 5 New Hampshire residents via mail on January 14, 2022.

If you have any questions, please do not hesitate to contact me.

Regards,

Gregory T. Parks

Enclosure

VAIL HEALTH

Return Mail Processing
PO Box 999
Suwanee, GA 30024

January 14, 2022

[redacted]

Re: Notice of Data Security Incident at Kronos

Dear [redacted]:

We are writing to notify you of a recent data security incident at Kronos, an outside timekeeping and payroll software vendor used by Vail Health. At this time, we have no suggestion from Kronos or any other source that your personal information has been accessed or used inappropriately, but we are sending this letter out of an abundance of caution to share with you what we know about what happened, what information Kronos has, what we have done, and what you can do to protect your continued privacy.

What Happened?
As you may know, Kronos is currently experiencing a global computer system outage due to a ransomware attack. Incidents like this sometimes result in access to or theft of personally identifying information. We currently do not know whether that happened in this case.

Since learning about the data security incident, we have asked Kronos to confirm whether any personal information was viewed or taken by an unauthorized party. To date, Kronos has not confirmed one way or the other whether any information was compromised. Although at this time we have not received any information that would suggest that your information was viewed or taken, we are sending this notice to advise you of the situation and offer some resources to help you protect your privacy.

What Information Was Involved?
While we have no indication that your personal information was accessed or used inappropriately, information in the Kronos systems includes your name, address, date of birth, social security number, salary, bank account information for direct deposit, W-2 and W-4 information. It also contains the information of dependents and beneficiaries including names, date of birth, and social security numbers.

What We Are Doing
Vail Health is committed to maintaining the privacy and security of your information and is taking this data security incident very seriously. Since learning of the incident, we have been taking steps to determine the data involved, details of the incident, and Kronos' plan to prevent reoccurrence. We will continue to follow up with Kronos to determine whether any of your information was affected and if we get confirmation that it was compromised, we will inform you promptly. Our

contracts with Kronos have always required Kronos to keep our employee information confidential and to have security procedures in place to minimize data security incidents, and we will continue to take steps to ensure that data held by Kronos on our behalf is adequately secured.

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorks℠. 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: April 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- 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 (888) 397-0018 by **April 30, 2022.** Be prepared to provide engagement number as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 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.

---

* 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.

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 (888) 397-0018. 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 12 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.

What You Can Do
There are several steps you can take to protect your continued privacy and be sure that your information is not used improperly, all of which are a good idea in any event. Enroll in the credit monitoring that we have offered you through this letter. This will enable you to get alerts about any efforts to use your name and social security number to establish credit and to block that credit from being established if you were not the one who initiated it.

Carefully review statements sent to you by your bank, credit card company, or other financial institutions, as well as government institutions like the IRS. Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.

The attached Reference Guide describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps.

For More Information
If you have questions or concerns not answered by this letter, please call (888) 397-0018.

Please know that Vail Health takes this matter very seriously, and we apologize for any concern and inconvenience this may cause you.

Sincerely,

Amanda Veit
Chief Operations Officer & Chief Nursing Officer

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For 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 200001, 202-727-3400, www.oag.dc.gov

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with 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. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For 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

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For 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

For Rhode Island Residents: 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.