30084

21 July 2023

[Original First Name] [Original Last Name]
[Original Address 1]
[Original Address 2]
[Original City], [Original State]
[Original Zip Code]

***RE: NOTICE OF DATA BREACH AND STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION***

Dear Valued HAVI Team Member,

We here at Vitality, a vendor that HAVI engaged to provide employee wellness services, are writing to inform you that we were recently impacted by a cybersecurity vulnerability in a third-party file transfer software we use called MOVEit. This is a widespread incident that has impacted hundreds of companies and state agencies that use MOVEit for exchanging business and banking information. Based on our investigation, it appears that some current and former HAVI colleagues may have had personal information impacted by this incident.

Please read below for additional information about what happened, the steps that are being taken to remediate this incident, as well as steps you can take to protect your information.

**What happened**
Based on our investigation and communications with MOVEit, we learned that MOVEit experienced a security vulnerability on May 30, 2023. Our internal security personnel identified this risk at approximately 11:30 a.m. Central Standard Time on June 1. Within minutes of becoming aware of the vulnerability, we immediately disconnected the MOVEit software server. This prevented all public access to the server and removed the known exploitable risk.

After reviewing the incident, we identified a two-hour span in which the vulnerability allowed the unauthorized third party to access the server that utilizes the MOVEit software. We took immediate action and temporarily disabled access to MOVEit to protect our members' data privacy and began forensics investigations to evaluate any impact. On June 12, 2023, we notified HAVI that we had confirmed a cybersecurity incident impacting HAVI employees and their personal information had occurred.

**What information was involved**
Based on our investigation, the personal information involved includes first and last name, social security numbers (which may be considered "protected health information" in this context) and, in some cases (but not all) may also include date of birth and some demographic information (such as gender).

**What we are doing**
To protect against similar attacks, Vitality has implemented various security changes to strengthen our systems against potential intrusions. In addition, we are cooperating with HAVI as it conducts additional assessment of our technical security measures to ensure that we have been providing and will continue to provide the security measures promised to HAVI and to help ensure this type of incident does not happen again. We are also taking additional steps to improve our security mechanisms. HAVI is also reviewing their own internal policies, procedures, and processes related to supply chain cybersecurity risk management to help ensure their vendors are properly protecting personal information and are only provided personal information in a very limited capacity. This review will be in addition to the HAVI's regular and ongoing reviews of their policies and procedures. HAVI continues to evaluate ways to enhance protection your personal information.

In addition, you are being provided two years of free identity theft protection and credit monitoring through Experian. Please see below for more information.

**What you can do**

As with any data security incident, we encourage you to continue to be vigilant about monitoring your personally identifiable information, in particular your credit report information and financial accounts, to protect against fraudulent activity. Please also take care and attention when submitting tax returns to protect against possible fraudulent submissions made on your behalf.

To assist you with monitoring your credit during this time you are entitled to, free of charge, two years' worth of identity theft protection and credit monitoring through Experian. In order to enroll in your complimentary membership, **we need you to contact Experian no later than 10/31/2023 by visiting https://www.experianidworks.com/credit, and providing the following activation code: [Activation code ].** Please review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further details on how to activate your complimentary 24-month membership of Experian's® IdentityWorks SM, as well as additional steps you can take to protect your information.

**For More Information**

We sincerely regret the concern this may cause, and deeply appreciate your support as we work to resolve it. Should you have questions or concerns regarding this matter, please do not hesitate to contact your HAVI point of contact Jen Sitrick at jen.sitrick@havi.com. Additionally, you can reach out to Experian at (800) 984-8152 and for Spanish at (800) 984-8308 between the hours of 6 a.m. to 8 p.m. PT and Saturday through Sunday from 8 a.m. to 5 p.m. PT (excluding major US holidays). Please be prepared to reference engagement number B090569 when speaking to an agent.

Sincerely,

**Lauren Prorok**
SVP, General Counsel
Vitality Group

**STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION**

To help protect your identity, we are offering a complimentary 24-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**: **October 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **[activation code]**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-901-4630 by October 31, 2023. Be prepared to provide engagement number **B096642** 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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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 833-901-4630. 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.

*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.

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service,
P.O. Box 105281, Atlanta, GA 30348. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 105851 | P.O. Box 9532 | P.O. Box 1000 |
| Atlanta, GA 30348 | Allen, TX 75013 | Chester, PA 19016 |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-916-8800 |
| www.equifax.com | www.experian.com | www.transunion.com |

**Fraud Alert:** You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, or obtain more information regarding fraud alerts, contact any of the three credit reporting agencies identified above. You also may contact the Federal Trade Commission ("FTC") as identified below for more information on fraud alerts.

**Security Freeze:** You may want to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. Under Federal law, there is no charge to place, lift, or remove a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies as identified above or the FTC as identified below. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

**Additional Free Resources:** We advise that you remain vigilant for events of fraud or identity theft by reviewing your account statements and monitoring credit reports closely to detect any errors or unauthorized activity resulting from this event. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.
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 FTC and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You may also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

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

Additional Information for Residents of:

**Iowa:** You may report suspected identity theft to local law enforcement and/or the Iowa Attorney General at Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319; (515) 2815164; www.iowaattorneygeneral.gov .

**New York:** You can obtain information from the New York State Office of the Attorney General or the New York Department of State Division of Consumer Protection about how to protect yourself from iden tity theft and tips on how to protect your privacy online. The Attorney General's office can be reached at: 1 -800 -771-7755; https://ag.ny.gov. The Division of Consumer Protection can be reached at: 1 -800 -697-1220; http://www.dos.ny.gov/consumerprotection .

**North Carolina:** You can obtain information from the North Carolina Attorney General's Office about preventing identity theft at: North Carolina Attorney General's Office, 9001 Mail Service Centre, R aleigh, NC 27699; 1-877- 566-7226; www.ncdoj.gov.

**Oregon:** You may report suspected identity theft to law enforcement, the FTC and/or the Oregon Attorney General at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301 -4096; 1-877-877-9392; www.doj.state.or.us.