Taft/

July 17, 2023

VIA U.S. MAIL
CONFIDENTIAL

Consumer Protection & Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Vitality Group, LLC

To Whom It May Concern:

In accordance with New Hampshire Revised Code §359-C:19, et. seq., I am providing the following notice of a security incident on behalf of our client, The Vitality Group, LLC ("Vitality"), which is writing on behalf of Alert Holding Company, Inc.

NAME AND CONTACT INFORMATION OF THE PERSON REPORTING THE BREACH;

Name:	Zenus Franklin
Position:	Outside Counsel for Vitality
Company	Taft Stettinius & Hollister, LLP
E-mail:	zfranklin@taftlaw.com
Address:	40 N. Main Street, #900 Dayton, Ohio 45423
Telephone number:	937.245.6864

NAME AND ADDRESS OF THE BUSINESS THAT EXPERIENCED THE BREACH, AND THE TYPE OF BUSINESS; OWNER OF THE PERSONAL INFORMATION;

Vitality, 120 S. Riverside Plaza, Suite 400 is a business-to-business vendor that provides employee benefit services, such as wellness services, to the Data Owner. Vitality experienced the security incident.

The Data Owner of the personal information subject to this security incident is Alert Holding Company, Inc. Vitality is a third-party vendor of the Data Owner.

A GENERAL DESCRIPTION OF THE BREACH, INCLUDING THE DATE(S) OF THE BREACH, WHEN AND HOW THE BREACH WAS DISCOVERED, AND ANY REMEDIAL STEPS TAKEN IN RESPONSE TO THE BREACH;

Vitality, and hundreds of global companies and state agencies use a third-party file transfer program called MOVEit to transfer data necessary to conducting business. MOVEit experienced a security vulnerability on May 30, 2023.

The zero-day vulnerability became known in established security networks and channels late on May 31, 2023, and was specifically picked up and identified by internal security personnel on June 1, 2023 at approximately 11:30 am CST. Within minutes of becoming aware of the vulnerability, Vitality disconnected the MOVEit software server. This prevented all public access to the server and removed the known exploitable risk.

Vitality took immediate action and temporarily disabled access to MOVEit to protect Vitality's members' data privacy and began forensics investigations to evaluate any impact. Vitality's security team conducted a thorough forensic analysis to ensure that no other servers or systems inside of the broader Vitality network were impacted. Please note that the MOVEit server is isolated on Vitality's network, which prevents any lateral movement to other Vitality systems. Vitality applied all available patches provided by MOVEit which Vitality believes fixed the vulnerability as well as followed all recommendations published by MOVEit. As an extra precaution, Vitality implemented a password reset on every account that accesses the server, along with additional security measures. Vitality is continuing to monitor the situation carefully.

After reviewing the incident, Vitality identified a two-hour span in which the vulnerability allowed the unauthorized third party to access the server that utilizes the MOVEit software. Vitality confirmed during its investigation that the Data Owner's information may have been accessed by the unauthorized third party. Vitality notified the Data Owner of the security incident. Vitality then worked with the Data Owner to understand what personal information may be involved and to identify any affected individuals.

THE NUMBER OF STATE RESIDENTS AFFECTED BY THE BREACH;

Vitality's investigation identified 7 individuals with a New Hampshire address that may have been impacted.

A DETAILED LIST OF CATEGORIES OF PERSONAL INFORMATION SUBJECT OF THE BREACH;

While the information varied based on the individual at issue, the information involved in this incident was limited to

THE DATE(S) THAT NOTIFICATION WAS/WILL BE SENT TO THE AFFECTED STATE RESIDENTS;

July 17, 2023.

A TEMPLATE COPY OF THE NOTIFICATION SENT TO THE AFFECTED STATE RESIDENTS;

Please see attached a substantially similar template copy of the notification sent to the residents.

WHETHER CREDIT MONITORING OR IDENTITY THEFT PROTECTION SERVICES HAS BEEN OR WILL BE OFFERED TO AFFECTED STATE RESIDENTS, AS WELL AS A DESCRIPTION AND LENGTH OF SUCH SERVICES; AND

Credit monitoring and identity theft prevention services have been offered via Experian for

WHETHER THE NOTIFICATION WAS DELAYED DUE TO A LAW ENFORCEMENT INVESTIGATION (IF APPLICABLE).

No

Please let us know if you have any further questions.

Yours faithfully,

Zenus Franklin

[INSERT] July 2023

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

NOTICE OF DATA BREACH

Dear [Original First Name] [Original Last Name]:

We write to inform you of a recent data security incident that occurred on May 30, 2023, at Vitality. This letter notifies you of the incident and informs you about steps that you can take to help protect your personal information. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information.

Who is Vitality?
Vitality acts as a third-party service provider on behalf of your (or your spouse's or domestic partner's) employer. The employer uses Vitality to provide access to certain wellness programs as part of its employee benefits program.

What Happened?
Vitality, and hundreds of global companies and state agencies, use a third-party file transfer program called MOVEit to transfer data to conduct its business. MOVEit reported a security vulnerability on May 30, 2023, impacting the MOVEit software.

Vitality's 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, Vitality disconnected the MOVEit software server. This prevented public access to the server and removed the known exploitable risk.

After reviewing the incident, Vitality identified a two-hour span in which the vulnerability allowed an unauthorized third party to access the Vitality server that utilizes the MOVEit software and obtain certain information belonging to individuals.

What information was involved
The information involved in this incident was limited to

What we are doing
Once Vitality became aware of the incident, Vitality took immediate action and temporarily disabled access to MOVEit to protect our members' data privacy and began forensics investigations to evaluate any impact. Vitality is also partnering with Experian to offer of complementary credit monitoring to affected members whose Social Security numbers were involved in this incident. A description of the benefits and enrollment instructions for the complimentary credit monitoring services is provided below.

What you can do
We encourage you to consider the following recommendations to protect your personal information:

- Register for Credit Monitoring Services: We have arranged for Experian to provide you with of complimentary credit monitoring and identity theft prevention services. **Enrollment instructions, including the deadline to enroll, is included with this letter.**

- Identity Protection: If you are concerned about identity theft, you can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit. Please read the information below or visit vitalitygroup.com/IDProtection for additional information on how to do so.

- Review Your Accounts for Suspicious Activity. We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.

- Order a Credit Report. If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.

- Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus. You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's websites at www.IdentityTheft.gov and www.ftc.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

  You may contact the nationwide credit reporting agencies at:

Equifax (800) 525-6285 P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com	Experian (888) 397-3742 P.O. Box 9701 Allen, TX 75013 www.experian.com	TransUnion (800) 916-8800 Fraud Victim Assistance Division P.O. Box 2000 www.transunion.com

- Additional Rights Under the FCRA. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here.

  Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcfp_consumerrights-summary_2018-09.pdf; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, N.W., Washington, DC 20552.

- Request Fraud Alerts and Security Freezes. You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult

for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax	Experian	TransUnion
(800) 349-9960	(888) 397-3742	(888) 909-8872

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

- For Maryland Residents. You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 576-6300, www.marylandattorneygeneral.gov.

- For New York Residents. You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755 (toll-free), 1-800-788-9898 (TDD/TTY toll-free line), https://ag.ny.gov/, and at: Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, Phone: (212) 416-8433, https://ag.ny.gov/internet/resource-center.

- For North Carolina Residents. You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov.

- For Residents of Oregon. You may report suspected identity theft to law enforcement, including the Office of the Oregon Attorney General and the FTC. Contact information for the FTC is included in your notice. The Office of the Oregon Attorney General can be reached: (1) by mail at 1162 Court St. NE, Salem, OR 97301; (2) by phone at (877) 877-9392; or (3) online at https://www.doj.state.or.us/.

- For Rhode Island Residents. You can obtain information about avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150, South Main Street, Providence, RI 02903, (401)-274-4400, www.riag.ri.gov. As it pertains to your (or your spouse's or domestic partner's)_ employer, information pertaining to approximately 1 Rhode Island resident was involved in this incident. You have the right to obtain a police report, and to request a security freeze (charges may apply), as described above.

- For Washington, D.C. Residents. You can obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202)-727-3400, www.oag.dc.gov. You have the right to request a security freeze (without any charge) as described above.

For More Information
Again, we sincerely regret that this incident has occurred. If you have any questions, please contact us at

Sincerely,

Lauren Prorok
SVP, General Counsel
Vitality Group

YOUR 24 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

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.