



ZENUS FRANKLIN
937.245.6864
zfranklin@taftlaw.com

August 22, 2023

VIA EMAIL
CONFIDENTIAL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: The Vitality Group, LLC

To Whom It May Concern:

In accordance with Maryland Code Ann. Com. Law §14-3501, 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 Guiding Eyes for the Blind.

NAME AND CONTACT INFORMATION OF THE PERSON REPORTING THE BREACH;

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

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

The Vitality Group, LLC (“Vitality”), 120 S. Riverside Plaza, Suite 400, Chicago, IL, 60606 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 Guiding Eyes for the Blind. 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 owned by Progress Software to transfer data necessary to conducting business. MOVEit was a victim of a cyber-security incident on May 30, 2023 when an unauthorized third party illegally gained access to Vitality's server which uses the MOVEit Software and may have downloaded data, including personally identifiable information. A Russian ransomware gang named "Clop" claimed responsibility for this incident.

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 Vitality's 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 (e.g., only allowing connections from approved Public IP addresses, known as an "IP AllowList" or IP "Whitelist" etc.). 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 has since worked with the Data Owner to understand what personal information may have been at risk and to identify and notify any affected individuals.

THE NUMBER OF STATE RESIDENTS AFFECTED BY THE BREACH;

Vitality's investigation identified 2 individuals with a Maryland address that may have been impacted. In the event that Vitality determines any additional Maryland residents are impacted, Vitality shall update this notice accordingly.

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

SSN and first name and last name.

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

Data Owner originally provided preliminary notice to its potentially affected employees on June 30, 2023. Notifications will be sent by Vitality, on behalf of the Data Owner, on August 22, 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 potentially affected individuals.

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 24 months.

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

No



[insert] 2023

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

Dear [Original First Name] [Original Last Name]

RE: IMPORTANT SECURITY NOTIFICATION. PLEASE READ THIS ENTIRE LETTER.

We are writing to inform you of a recent security incident at Vitality, our health and wellness engagement platform, which is made available to you through your employer. As a result, your PII (Personally Identifiable Information) may have been potentially exposed. This notification is being sent pursuant to your state's applicable data security law(s).

What happened

A third-party file transfer program called MOVEit owned by Progress Software was used by Vitality to transfer necessary data. MOVEit was a victim of a cyber security incident that occurred on May 30, 2023, when an unauthorized third party illegally gained access to Vitality's server which uses the MOVEit Software and downloaded data, which included PII (Personally Identifiable Information). A ransomware gang named "Clop" claimed responsibility for this incident.

Vitality identified this risk at approximately 11:30 a.m. Central Standard Time on June 1, 2023. Within minutes of becoming aware of the vulnerability, Vitality disconnected the MOVEit software server. This prevented all public access to the server, thereby shutting down connectivity and removed the known exploitable risk. What was the impact?

After investigating 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 took immediate action and temporarily disabled access to MOVEit to protect our members' data privacy and began forensics investigations to evaluate any impact. The findings show that 171 individuals' data was compromised.

What information was involved

The information potentially at risk could have included your name and Social Security number.

What we are doing

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. Vitality applied all available patches provided by MOVEit which 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 (e.g., only allowing connections from approved Public IP addresses, known as an "IP AllowList" or IP "Whitelist" etc.). Vitality is continuing to monitor the situation carefully.

Vitality also partnered with Experian to offer 2 years of credit monitoring to affected members with compromised private information.

What you can do

While we have received no reports or indication of such activity, the risks related to unauthorized use of a Social Security number may include identity theft, financial fraud, and tax fraud. Please 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 in this effort, we have provided complimentary credit monitoring and identity theft prevention services through Experian. If you are concerned about identity theft, please sign up for the complimentary monitoring and protection services by following the instructions enclosed or provided below from Experian. The deadline to sign up for this complimentary monitoring and protection service is October 31, 2023.

Other important information

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 report. Please visit vitalitygroup.com/IDProtection

For More Information

Again, we sincerely regret that this incident has occurred. On the following pages, we've also included important information about free resources and agencies to assist you, if necessary. If you have any questions, please contact us at 833-901-4630.

Contact: The Vitality Group, LLC
Email: Wellness@powerofvitality.com
Telephone: 1-877-224-7117 & 1-800-828-9572
Address: Vitality Group
120 S Riverside Plaza
Suite 400
Chicago, IL 60606

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® 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: 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 ExtendCARETM:** 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.

Steps You Can Take to HELP Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

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 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. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
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 one year. 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, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies. You may obtain a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322- 8228 or by completing an Annual Credit Request Form at: <https://consumer.ftc.gov/> and mailing to:

Annual Credit Report Request Service,
P.O. Box 1025281
Atlanta, GA 30348-5283

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001

1-877-566-7226

1-401-274-4400

oag.dc.gov
1-202-727-3400

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