



ZENUS FRANKLIN
937.245-6864
zfranklin@taftlaw.com

July 17, 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 Concordia Plan Services.

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, #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 Concordia Plan Services. Vitality is a third-party vendor of the Data Owner. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, neither Vitality nor Data Owner waives any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

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 have been at risk and to identify any affected individuals.

THE NUMBER OF STATE RESIDENTS AFFECTED BY THE BREACH;

Vitality’s investigation identified 7 individuals affiliated with Data Owner with a Maryland address that may have been impacted. In the event that Vitality determines any additional Maryland residents are impacted, Vitality may update this notice accordingly.

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

The personal information of individuals affiliated with Data Owner that could have been subject to unauthorized access includes the following: first and last name and Social Security number.

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

On July 17, 2023 Vitality provided written notice of this event to potentially impacted individuals on Data Owner's behalf, including approximately 7 Maryland residents.

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 24 months.

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

No

OTHER

Additionally, Vitality, on behalf of Data Owner, is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft and fraud to law enforcement and their credit reporting company. Vitality, on behalf of Data Owner, also is providing individuals with information on how to place a fraud alert and credit freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.



[INSERT] July 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 contacting you regarding a data security incident that has occurred on May 30, 2023 at Vitality. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident.

What happened

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.

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 all 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 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.

What information was involved

The information potentially exposed included your first and last name, social security number and date of birth. Also included was an indication that you may have participated in a wellness activity for which you could earn Vitality points. For example, the exposed information may indicate the date you registered with a virtual care service provider or the date that you or a member of your family received an eye exam. No other information pertaining to your health care or medical condition was exposed.

What we are doing

Vitality is partnering with Experian to offer two years of credit monitoring to affected members with compromised Social Security numbers.

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

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT**Place a 90-day fraud alert on your credit file**

An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax

1-800-525-6285
www.equifax.com

Experian

1-888-397-3742
www.experian.com

TransUnion

1-800-680-7289
www.transunion.com

Place a security freeze on your credit file

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

Order your free annual credit reports

Visit www.annualcreditreport.com or call 877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Manage your personal information

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information. It is also a good idea to review any Explanation of Benefits you receive from your health plan to confirm that the services described were received.

Use tools from credit providers

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

Obtain more information about identity theft and ways to protect yourself

1. Visit <http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html> for general information regarding protecting your identity.
2. The Federal Trade Commission has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For More Information

Again, we sincerely regret that this incident has occurred. 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.

Additional Information for Residents of Certain States

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.