

Taft/

NH DEPT OF JUSTICE
JUL 3 '23 PM 12:03

June 30, 2023

VIA FEDERAL EXPRESS
CONFIDENTIAL

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

RE: The Vitality Group, LLC

To Whom It May Concern:

I am providing notice of a security incident on behalf of our client, The Vitality Group, LLC ("Vitality"), which is writing on behalf of Kuecker Pulse Integration, LP ("KPI") to notify you of a recent data security incident in accordance with New Hampshire Revised Code §359-C:19, et. seq.

NAME AND CONTACT INFORMATION OF THE PERSON REPORTING THE BREACH

<u>Name:</u>	Scot Ganow
<u>Position:</u>	Outside Counsel to Vitality
<u>Company:</u>	Taft Stettinius & Hollister, LLP
<u>E-mail:</u>	sganow@taftlaw.com
<u>Address:</u>	40 North Main Street, Suite 900 Dayton, Ohio 45423
<u>Telephone number:</u>	937-641-2041



SCOT GANOW
937.641.2041
sganow@taftlaw.com

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. On or about May 31, 2023, Progress Software – the company responsible for the MOVEit file transfer program – released an advisory announcing a vulnerability associated with MOVEit. The vulnerability allowed an unauthorized third party to access, and download information on the Vitality server that utilizes the MOVEit software. On June 1, 2023, Vitality's internal security personnel learned of the MOVEit vulnerability. In response, Vitality disconnected its MOVEit server to prevent all public access thereto and remove the known exploitable risk. Vitality then commenced an internal investigation through which internal security personnel identified a two-hour time period during which an unauthorized third-party leveraged the MOVEit vulnerability to access the Vitality server that utilizes the MOVEit software and download information stored there. On June 11, 2023, Vitality informed KPI that data belonging to certain current / former employees and their spouses appeared to have been impacted in connection with the incident. KPI takes the privacy and security of all information very seriously and, upon receipt of this information, began working diligently with Vitality to provide notification to impacted individuals. Vitality and KPI are aware of no evidence of the misuse of any impacted information.

TYPE OF INFORMATION AND NUMBER OF STATE RESIDENTS NOTIFIED

The data sets potentially accessible by the malicious actor(s) responsible for this incident included individuals' . On 30 June 2023 Vitality – on behalf of KPI – notified 2 New Hampshire residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to potentially impacted individuals is included with this correspondence.

STEPS TAKEN RELATING TO THE INCIDENT

Vitality learned of the MOVEit vulnerability on June 1, 2023 and promptly executed its incident response processes, including but not limited to taking measures to isolate the MOVEit server, apply available software patches, implement password resets, commence a forensic investigation, reach out to law enforcement, and notify its corporate customers, among other actions.

Vitality is also partnering with Experian to offer of credit monitoring and identity theft protection services to impacted individuals. Those services include credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.



SCOT GANOW
937.641.2041
sganow@taftlaw.com

CREDIT MONITORING

Credit monitoring and identity theft prevention services will be offered via Experian for 24 months.

Vitality and KPI remain dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me as provided above.

Sincerely,

Scot Ganow



VITALITY GROUP, INC. © 2023

[INSERT] June 2023

[Original First Name] [Original Last Name]
[Original Address1]
[Original Address2]
[Original City], [Original State]
[Original Zip Code]

Dear [Original First Name] [Original Last Name]

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

The Vitality Group, LLC ("Vitality") is writing to notify you of a recent data security incident that appears to have impacted your personal information.¹ Please read this letter carefully as it contains details regarding the incident and steps that you can take to help protect your personal information.

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. On or about May 31, 2023, Progress Software – the company responsible for the MOVEit file transfer program – released an advisory announcing a vulnerability associated with MOVEit. The vulnerability enabled unauthorized, third-party criminal actors to download information stored within the MOVEit program.

On June 1, 2023, Vitality's internal security personnel learned of the MOVEit vulnerability. In response, Vitality disconnected its MOVEit software server to prevent all public access thereto and remove the known exploitable risk. Vitality then commenced an internal investigation through which internal security personnel identified a two-hour time period during which an unauthorized third-party leveraged the MOVEit vulnerability to access the MOVEit software server and download information stored there.

On June 11, 2023, Vitality informed Kuecker Pulse Integration, LP ("KPI") that data belonging to certain current / former employees and their spouses appeared to have been impacted in connection with the incident. KPI takes the privacy and security of all information very seriously and, upon receipt of this information, began working diligently with Vitality to provide notification to impacted individuals. Vitality and KPI are aware of no evidence of the misuse of any impacted information.

What Information Was Involved

This incident involved
exposed to an unauthorized third-party.

which may have been

¹ Kuecker Pulse Integration, LP ("KPI") – the current or former employer of you or your spouse – provided Vitality with the potentially impacted information in connection with its engagement of Vitality to provide wellness services to you.



What We Are Doing

As soon as Vitality discovered the incident, Vitality took the steps described above. Vitality is also partnering with Experian to offer two years of credit monitoring and identity theft protection services to impacted individuals.

What You Can Do

While Vitality has received no reports or indication of misuse of impacted information, 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 personal 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 are providing you with access to complimentary credit monitoring and identity theft prevention services through Experian. Please sign up for these complimentary services by following the enclosed instructions. The deadline to sign up for these services is October 31, 2023.

Other Important Information

You can follow the recommendations on the following page to help protect your personal 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. Please visit

For More Information

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

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 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:

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. Be prepared to provide engagement number 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>.

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
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

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