



SCOT GANOW
937.641.2041
sganow@taftlaw.com

July 5, 2023

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Mr. Brown:

I am providing notice of a security incident on behalf of our client, The Vitality Group, LLC ("**Vitality**"), 120 S. Riverside Plaza, Suite 400, Chicago, Illinois. Vitality is a business-to-business vendor that provides employee benefit services, such as wellness services, to bioMérieux, Inc. ("**bioMérieux**") and other companies. We are writing to notify you of a data security incident experienced by Vitality involving the personal information of Maryland residents for which bioMérieux acts as the data owner.

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 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, and confirmed that bioMérieux's information may have been accessed by the unauthorized third party. Vitality provided initial notice of the incident directly to bioMérieux on June 5, 2023. Vitality then worked with bioMérieux to

understand what personal information may have been at risk and to identify any affected individuals. In the interim and out of an abundance of caution, on June 15, 2023, bioMérieux issued an advisory to potentially impacted individuals stating its awareness of an incident involving Vitality, and that it was investigating the same; however, bioMérieux did not yet have specifics as to the individualized personal information that may have been involved. On June 16 and June 20, 2023, Vitality provided bioMérieux with information indicating that the Vitality incident may have involved personal information of 195 Maryland residents for which bioMérieux acts as the data owner, including name, date of birth, social security number, and health-related information.

All of the individuals who may potentially have been impacted by the incident will be notified by U.S. mail on July 6, 2023. A template of that notice is attached to this correspondence, and such notices will not be delayed as a result of any law enforcement activities. Additionally, Vitality is providing all potentially impacted individuals with twenty-four months of credit monitoring and identity theft insurance services administered through Experian.

Vitality will supplement this notice, if necessary, with any additional significant facts discovered subsequent to this correspondence. Please do not hesitate to contact me if you have any questions or if you require additional information concerning this matter.

<u>Name:</u>	Scot Ganow, Esq., CIPP/US
<u>Company:</u>	Taft Stettinius & Hollister, LLP
<u>Position:</u>	Outside Counsel to Vitality
<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

Sincerely,

A handwritten signature in black ink, appearing to read "Scot Ganow", written in a cursive style.

Scot Ganow

ATTACHMENT:
Template Individual Notice

NOTICE OF DATA BREACH**MEMBER FIRST NAME/LAST NAME****MEMBER ADDRESS**Dear **(MERGE MEMBER FIRST NAME)**,

On June 15, 2023, we provided an initial notice (email and a letter) to you about a data security breach involving the unauthorized disclosure of personal information that a bioMérieux vendor, Vitality Group, recently reported to us. Today we are providing an update regarding that data breach and categories of information impacted.

WHAT HAPPENED?

Vitality recently reported that, on June 1, 2023, it became aware of a critical security vulnerability in its IT system infrastructure resulting from the exploitation of a vulnerability in its instance of a widely used file transfer application, MOVEit Transfer. Upon becoming aware of the vulnerability, Vitality states that it immediately took action to remove the exploitable risk and that it initiated an evaluation of the vulnerability.

Based on its evaluation, Vitality concluded that there had been unauthorized access to its member database, including suspicious file download activity. Vitality subsequently determined that files with personal information belonging to Vitality members associated with bioMérieux were compromised.

WHAT INFORMATION WAS INVOLVED?

On June 20, 2023, Vitality provided bioMérieux with updated information regarding affected bioMérieux Vitality members. Based on currently available information, we can confirm that the member data accessed included social security numbers, health information, first names and last names, and other personal information. Impacted individuals may include current and former members, as well as family members.

Based on information provided to bioMérieux by Vitality as of the date of this Notice, it has been determined that the following categories of your personal information were compromised as part of this breach:

MERGE CATEGORICAL EXPLANATION HERE

Term	Description
SSN	Social Security Number
DOB	Date of Birth
HI - Claims	Health Information. Vitality receives medical procedure codes for eligible member claims on bioMerieux's medical plan
HI - Screenings	Health Information. Vitality receives screening results for eligible members who complete their Vitality Check screenings though Health Advocate's on-site events or screening vouchers.

WHAT ARE WE DOING?

bioMérieux takes the protection of personal information seriously and immediately initiated a review of information relating to the data breach as soon as it was made available by Vitality. bioMérieux has stopped sharing team member personal data with Vitality while Vitality's investigation and bioMérieux's review of the data breach are ongoing. bioMérieux is continuing to monitor this data breach and will provide a further update if there is any significant development.

While this data breach does not involve any bioMérieux systems and given that its review is still ongoing, bioMérieux is providing this official notice of data breach in the interest of transparency and out of an abundance of caution.

WHAT CAN YOU DO?

As a reminder, Vitality has partnered with Experian to offer two years of credit monitoring and identity theft insurance to impacted members and their impacted family members. Vitality emailed information on June 16, 2023, regarding how to access credit monitoring and related services.

FOR MORE INFORMATION

If you did not receive the credit monitoring information from Vitality, or if you have additional questions regarding credit monitoring and related services, Vitality has established a customer care hotline operated by Experian. You may contact the hotline at (800) 828-9572 with questions regarding the vulnerability, credit monitoring, identity theft protection, and related matters.

Please also review the information enclosed with this letter for further information on steps you can take to protect your information.

The bioMérieux HR Support Hub team members are also available at (919) 620-2527 and HRHub@biomerieux.com to answer bioMérieux benefits program-specific questions. BioFire Defense, Transgene and ABL team members receiving this letter should reach out to their respective HR Business Partners with questions.

An FAQ with additional information is available by scanning this [QR Code](#). Please bookmark this web page for future reference, as it will be updated periodically as more information becomes available.

Erica Ruffin
Senior Vice President
Human Resources, North America

Steps You Can Take to Further 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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Additional information for the FTC is provided below:

Federal Trade Commission
(202) 326-2222
<https://www.ftc.gov/>
600 Pennsylvania Avenue, NW
Washington, DC 20580

- **Obtain and Monitor Your Credit Report**

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 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 can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>, or you can elect to purchase a copy of your credit report, for a fee, 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
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

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, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze

- In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must

separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze. For more information, please visit <https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts> and <https://www.identitytheft.gov/#/CreditBureauContacts>.

- **Additional Information for DC, MD, NY, NC, and RI Residents**

If you are located in the District of Columbia, Maryland, New York, North Carolina, or Rhode Island, you may wish to report any fraudulent activity or any suspected incidence of identity theft to your state attorney general or relevant state agency. Additional information is provided below:

District of Columbia

Office of the Attorney General for the District of Columbia
(202) 727-3400
<https://oag.dc.gov/>
400 6th Street NW
Washington, D.C. 20001

Maryland

Office of the Attorney General for Maryland
(410) 528-8662
<https://www.marylandattorneygeneral.gov/>
200 St. Paul Place
Baltimore, MD 21202

New York

Office of the New York State Attorney General
1 (800) 771-7755
<https://ag.ny.gov/>
The Capitol
Albany, NY 1222

New York Department of State Consumer Protection Board
1 (800) 697-1220
<https://dos.ny.gov/>
5 Empire State Plaza, Suite 2101
Albany, NY 12223

North Carolina

Office of the North Carolina State Attorney General
(877) 5-NO-SCAM
<https://ncdoj.gov/>
114 West Edenton Street
Raleigh, NC 27603

Rhode Island

Office of the Rhode Island State Attorney General
(401) 274-4400
<https://riag.ri.gov/>
150 South Main Street
Providence, RI 02903