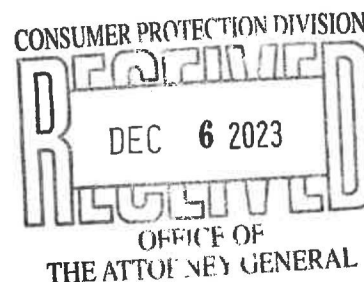


RE: BREACH NOTIFICATION

ADDRESSED TO:

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



16 November 2023

Dear Sir/Madam,

I herewith file the following notification, detailing how the MOVEit breach has affected Spectris, Inc and its businesses in the US that are covered under the relevant benefit and health care contracts signed by Spectris, Inc..

NAME AND CONTACT INFORMATION OF THE PERSON REPORTING THE BREACH

<u>Name:</u>	Danielle Folkersma
<u>Position:</u>	Group Privacy Counsel
<u>E-mail:</u>	Danielle.folkersma@spectris.com
<u>Address:</u>	Spectris Plc, Melbourne House, 5th Floor, 44 46 Aldwych, London, WC2B 4LL, United Kingdom
<u>Telephone number:</u>	+31641313742

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 Spectris, Inc., the Data Owner of the personal information subject to this security incident. Spectris plc is the parent company of Spectris, Inc. Vitality was the business that experienced the security incident.

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 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 Spectris, Inc.'s information may have been accessed by the unauthorized third party. Vitality notified Spectris, Inc. of the security incident. Vitality then worked with Spectris, Inc. to understand what personal information may have been at risk and to identify any affected individuals.

While investigations by Vitality were still ongoing, Spectris, Inc. immediately informed its businesses, who in turn informed their employees (hereafter referred to as 'Spectris employees'), in order to mitigate risk through awareness. Once Vitality understood the types of personal data and employees affected, they informed the affected employees by letter, offering complimentary credit monitoring and identity theft prevention services (provided through Experian).

Spectris plc (Head Office in the UK) was made aware of the breach by Spectris Inc. and following this notification, its Cyber Security and Data Protection teams started further assessments on the circumstances, the risks involved and State breach notification laws.

In the meantime, Spectris, Inc. contacted their other benefit and health insurance providers to review whether they were also impacted by the MOVEit incident. To date,

17 out of the 18 vendors have confirmed that Spectris, Inc.'s data has not been impacted. One vendor is still investigating the situation and is unable to provide any details until their investigation has been completed. Spectris, Inc. does not have any insight as to when their investigation will be closed but will report it to the relevant State authorities if required once the findings of the investigation have been shared.

THE NUMBER OF STATE RESIDENTS AFFECTED BY THE BREACH;

Spectris' investigation identified the following number of state residents per State (for which breach notification laws apply based on the circumstances) that may have been impacted through Vitality:

State	Number of Spectris employees/ State residents possibly impacted
Connecticut	1
Indiana	6
Louisiana	2
Massachusetts	166
Maryland	5
Maine	1
Missouri	4
North Carolina	13
New Hampshire	18
New Jersey	10
New York	19
Virginia	3

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

Information impacted through Vitality concerned social security numbers and contact information, such as name, phone number, address or email address of 1,237 Spectris employees across 41 US States. No private health information was at risk (HIPAA does not apply).

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

Letters to officially notify affected employees were sent by Vitality on or around 19 July 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 by Vitality.

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

Please let us know if you have any further questions.

Yours faithfully

Danielle Folkersma

Danielle Folkersma

Spectris Group Privacy Counsel

T[Company Logo]

[Return Address]

[Return Address]

[Date]

[Insert Recipient's Name]

[Insert Address]

[Insert City, State, Zip]

RE: Important Security Notification
Please read this entire letter.

Dear [Insert customer name]:

We are contacting you regarding a data security incident that has occurred on May 31, 2023 at Vitality. This incident involved your [First and last name] [Social Security Number] [date of birth] [PHI] [and other demographic information]. 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 31, 2023. You can read more about the vulnerability and its impact [here](#).

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

[First and last name]	[Social Security Number]	[Date of birth]
[PHI]	[other demographic information]	

What We Are Doing

Vitality is partnering with Experian to offer 2 years of credit monitoring to affected members with compromised PHI and/or Social Security numbers. You will receive a letter from Experian with a unique access code.

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 [ENROLLMENT DATE].

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. Please visit vitalitygroup.com/IDProtection

For More Information

Again, we sincerely regret that this incident has occurred. If you have any questions, please contact us at (800) 828-9572.

Contact: [COMPANY NAME]

Email: [EMAIL ADDRESS]

Telephone: [TELEPHONE NUMBER] & [TOLL FREE NUMBER]

Address: [COMPANY NAME]

[STREET ADDRESS]

[CITY, STATE & ZIP CODE]

Sincerely,

[Reporting Individual Name & Contact Information]

Commented [FZ1]: AL, CA, CO, FL, HI, MD, MI, NH, NY, OR, WA, WV, WY, PR require notice to include the company's contact information where individuals may inquire about breach. *Note that WY and PR specifically require a toll free number.

MO, NC, VT, VA require a telephone number that affected consumers may call for additional information, *if one exists*.

D.C. and FL require the company's address to be included in notice letter. CO (advises that the company's address be listed is not required)

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: [enrollment end date] (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [URL]
- Provide your activation code: [code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [customer service number] by [enrollment end date]. Be prepared to provide engagement number [engagement #] 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 [customer service number]. 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 ___ 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.