



SCOT GANOW
937.641.2041
sganow@taftlaw.com

July 5, 2023

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Brown:

I am providing notice of a security incident on behalf of my client, The Vitality Group, LLC ("Vitality").

NAME AND CONTACT INFORMATION FOR THE ORGANIZATION REPORTING THE BREACH – VITALITY GROUP

<u>Name:</u>	Scot Ganow
<u>Position:</u>	Outside Counsel of 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

NAME AND CONTACT INFORMATION FOR THE DATA OWNER – HERZING UNIVERSITY

<u>Name:</u>	Casey Vaughn
<u>Position:</u>	Outside Counsel for Herzing University
<u>Company:</u>	Armstrong Teasdale, LLP
<u>E-mail:</u>	cvaughn@atltp.com
<u>Address:</u>	7700 Forsyth Blvd., Suite 1800 St. Louis, MO 63108



SCOT GANOW
937.641.2041
sganow@taftlaw.com

<u>Telephone number.</u>	314.621.5070 ext. 7066
--------------------------	------------------------

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

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 Herzing University (Herzing). Vitality experienced the security incident.

The Data Owner of the personal information subject to this security incident is Herzing. Vitality, as a third party vendor of Herzing and the entity that experienced the incident, is making this report on behalf of Herzing. Vitality and Herzing may be contacted through their respective outside counsel at the information indicated above.

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 numerous other organizations, use a third-party file transfer program called MOVEit to transfer data necessary to conduct 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 potential 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.

The MOVEit server is isolated on Vitality's network, which Vitality believes prevents any lateral movement to other Vitality systems. Vitality applied all available patches provided by MOVEit, which it believes fixed the vulnerability, and followed all



SCOT GANOW
937.641.2041
sganow@taftlaw.com

recommendations published by MOVEit. As an extra precaution, Vitality implemented a password reset on every account that accesses the MOVEit 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 Vitality's server that utilizes the MOVEit software.

Vitality confirmed during its investigation that Herzing's information may have been accessed by the unauthorized third party. Vitality notified Herzing of the security incident. Herzing then worked with Vitality to understand whether and what personal information may have been at risk and to identify any affected individuals. Herzing provided notice to the individuals identified by Vitality as affected by the incident on July 5, 2023.

All individuals impacted by the incident are being offered 24-months of free Experian IdentityWorks 3B credit monitoring services.

THE NUMBER OF STATE RESIDENTS AFFECTED BY THE BREACH:

Vitality and Herzing's investigations identified 1 individual with a Maryland address that may have been impacted.

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

Based on the information provided by Vitality, Herzing believes the categories of personal and health-related information involved in this incident may include an individual's name, birthdate, government-issued identification number (i.e., social security number), home address, email address, home and work phone numbers, other general employment-related information (employment start date, etc.), gender, marital status, and benefits information such as member ID, group policy number, effective date of coverage, and subscriber identification number.

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

July 5, 2023



SCOT GANOW
937.641.2041
sganow@taftlaw.com

**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:**

Credit monitoring and identity theft prevention services offered through Experian have been offered free of charge to all impacted individuals for 24 months.

Please let us know if you have any further questions.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to inform you about a data security incident involving Vitality Group, LLC ("Vitality"), a wellness programs and services vendor to Herzing University ("Herzing"), which may have exposed some of your personal information, and to provide you with steps you can take to help protect your information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident and provide you with the opportunity to take advantage of the complimentary identity monitoring services described below.

What Happened

It is our understanding that Vitality, like numerous other organizations, uses a third-party file transfer program called MOVEit to transfer data necessary to conduct business. Vitality recently notified Herzing that MOVEit experienced a security vulnerability on May 30, 2023. It is our understanding that the vulnerability was specifically picked up and identified by Vitality's internal security personnel on June 1, 2023, at approximately 11:30 am CST. According to Vitality, they disconnected the MOVEit software server within minutes of becoming aware of the vulnerability. Vitality believes this prevented all public access to the server and removed the known exploitable risk.

Vitality informed us that after they took immediate action and temporarily disabled access to MOVEit, they began forensic investigations to evaluate any impact from the vulnerability. According to Vitality, the MOVEit server is isolated on Vitality's network, which prevents any lateral movement to other Vitality systems. Vitality informed us that it applied all available patches provided by MOVEit, which it believes fixed the vulnerability, as well as followed all recommendations published by MOVEit. Vitality also informed us that it implemented a password reset on every account that accesses the server. According to Vitality, it is continuing to monitor the situation carefully.

It is our understanding from Vitality that there was a two-hour span in which the vulnerability allowed an unauthorized third party to access the server that utilizes the MOVEit software. Vitality has informed us that information belonging or relating to Herzing employees and associated individuals may have been accessed by the unauthorized third party.

Vitality provided Herzing with initial notification of the security incident on June 2, 2023. Following this initial notification, Herzing immediately engaged in discussions with Vitality regarding the incident, and requested additional information from Vitality to begin its own analysis of the incident, including the type of information potentially involved and whether any Herzing employees or associated individuals were impacted. After analyzing the additional information provided by Vitality, on June 20, 2023, Herzing confirmed that the incident involved personally identifiable information and health-related information of Herzing employees and associated individuals. Since then, Herzing has continued to engage with Vitality regarding remediation efforts for impacted individuals, including credit monitoring being offered by Vitality.

What Information Was Involved

Based on the information provided by Vitality and our own analysis of the incident, the personal and health-related information involved in this incident may have included your name, birthdate, government-issued identification number (i.e., social security number), home address, email address, home and work phone numbers, other general employment-related information (for Herzing employees), gender, marital status, and benefits information such as member ID, group policy number, effective date of coverage, and subscriber identification number. Based on the information provided to us by Vitality, it does not appear that any diagnosis or treatment information was exposed.

What We Are Doing

Upon receiving notification from Vitality, Herzing requested information from Vitality regarding Vitality's investigation and mitigation of the incident. Herzing also undertook its own analysis of the incident with the help of legal counsel. Herzing is working with Vitality to ensure that appropriate regulatory and law enforcement officials are notified and able to investigate the matter. In addition, out of an abundance of caution, Herzing continues to monitor its own systems for any suspicious activity.

To help relieve concerns and attempt to mitigate the consequences of this incident on affected individuals, Vitality is offering all Herzing employees and associated individuals affected by the incident a complimentary twenty-four month membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. Activate IdentityWorks Credit 3B now in Three Easy Steps:

1. ENROLL by: <<b2b_text_6(activation deadline)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/credit>
3. PROVIDE the **Activation Code**: <<activation code s_n>>

For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary twenty-four month membership, please see the additional information provided in this letter. Please note that services will only be activated if you visit the website listed above and sign up using the membership number provided in this letter.

What You Can Do

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection, details on how to place a fraud alert or a security freeze on your credit file, and details regarding the free identity monitoring services you are being offered.

For more information.

If you have questions, please call (866) 373-7160, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready. You may also write to Herzing at 275 W. Wisconsin Ave., Ste 210, Milwaukee, WI 53203, RE: Vitality Incident.

Protecting your information is important to us and we sincerely regret that this incident has occurred. We trust that the services being offered to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,



Shannon Grass
SVP Human Resources, Herzing University

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, and Maryland residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338). The Federal Trade Commission can also provide you with information about fraud alerts and security freezes.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain a police report if you are a victim of identity theft.

ADDITIONAL INFORMATION CONCERNING IDENTITYWORKS CREDIT 3B

To help protect your identity, Vitality is 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:** <<b2b_text_6(activation deadline)>> (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 s_n>>

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 **833-901-4630** by <<b2b_text_6(activation deadline)>>. Be prepared to provide engagement number <<b2b_text_1(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 ExtendCARE™:** 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.