CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN FARALLY
mfarally@c-wlaw.com

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

September 13, 2021

Via First Class Mail
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Data Breach Notification

To Whom It May Concern:

I serve as counsel for Williamson College of the Trades ("Williamson") and provide this notification to you of a recent data security incident. By providing this notice, Williamson does not waive any rights or defenses under New Hampshire law, including the data breach notification statute.

Williamson recently identified suspicious activity related to an employee email account. Upon discovery, Williamson immediately took steps to secure the relevant account and began investigating with the assistance of a third-party forensic specialists. The investigation confirmed that one employee email account was subject to unauthorized access on or around June 25, 2021. Upon confirmation of the unauthorized activity, Williamson immediately began an extensive manual review of the contents of the email account to determine the type of information contained within the account and to whom that information related. Williamson subsequently conducted a review of their internal files to confirm contact information for potentially impacted individuals so Williamson could provide written notice of the incident. Williamson's review has identified that the Social Security number of three (3) New Hampshire residents was contained within the impacted email account.

Williamson mailed notification to the affected individuals on September 10, 2021, and is providing one (1) year of complimentary credit monitoring and identity protection services. A copy of the notification letter is attached. Williamson is also reviewing its policies and procedures related to data security.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: 
Meghan S. Farally

Return Address Information

<<First Name>> <<Last Name >>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

Dear <<First Name>> <<Last Name >>:

Williamson College of the Trades ("Williamson") is writing to inform you of an incident experienced by our institution that may have involved your information described below. We take the privacy and security of all information in our care very seriously. While we have no evidence of misuse of any information as a result of this incident, we are providing you with information about the incident, our response, and steps you can take to better protect your information against the possibility of identity theft and fraud, should you feel it appropriate to do so.

What Happened: Williamson recently identified suspicious activity related to an employee email account. Upon discovery, we immediately took steps to secure the relevant account and began investigating with the assistance of a third-party forensic specialists. The investigation confirmed that one employee email account was subject to unauthorized access on or around June 25, 2021. Upon confirmation of the unauthorized activity, we immediately began an extensive manual review of the contents of the email account to determine the type of information contained within the account and to whom that information related. We subsequently conducted a review of our internal files to confirm contact information for potentially impacted individuals so we could provide written notice of the incident.

What Information Was Involved: The information contained in the email account may have included your name, in combination with your Social Security number.

What We Are Doing: Upon learning of this incident, we immediately performed a password reset and took steps to confirm the security of our systems. Additionally, we are notifying potentially impacted individuals and offering complimentary credit monitoring and identity protection services for 12 months.

What You Can Do: We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. You may also enroll in the complimentary credit monitoring and identity protection services we are making available to you. Additional information regarding how to enroll in the complimentary services is enclosed in the attached "Steps You Can Take to Protect Your Information."

For More Information: We understand you may have questions or concerns regarding this matter that are not addressed in this letter. Please contact Dr. Todd Zachary at [redacted] with any additional questions you may have

Williamson sincerely regrets any inconvenience or concern this incident may have caused you.

Sincerely,

Dr. Todd Zachary
Provost

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

TransUnion® *my*TrueIdentity provides you with the following key features:

- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- One year of unlimited access to your TransUnion® credit report and credit score.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible.[1]

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at [redacted] When prompted, enter the six-digit telephone passcode [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **December 31, 2021**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Monitor Your Accounts

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit [redacted] or call [redacted] 8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.).
2. Social Security number.
3. Date of birth.
4. Address for the prior two to five years.
5. Proof of current address, such as a current utility or telephone bill.
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card);

---

[1] (Policy limitations and exclusions may apply.)

and

7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.