

RECEIVED

APR 08 2024

CONSUMER PROTECTION

April 4, 2024

**VIA U.S. MAIL**

Attorney General John Formella  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: York County School of Technology – Incident Notification**

Dear Sir or Madam:

McDonald Hopkins PLC represents York County School of Technology (“York Tech”). I am writing to provide notification of an incident at York Tech that may affect the security of personal information of one (1) New Hampshire resident. By providing this notice, York Tech does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On or about April 26, 2023, York Tech experienced a network security incident that affected some operations. Upon experiencing the incident, York Tech partnered with cybersecurity experts and conducted a thorough investigation to understand the nature and scope of the event. After an extensive forensic investigation and manual review, on March 15, 2024, York Tech determined that on or about March 27, 2023, certain impacted files containing personal information may have been subject to unauthorized access or acquisition. The information potentially accessed includes full name, address, driver’s license number, Social Security number email username/password, medical information, and health insurance information. The type of impacted information varies by individual and not all elements were necessarily impacted. The information impacted for the one (1) New Hampshire Resident includes

. On March 29, 2024, York Tech determined the most recent contact information of the impacted individuals.

York Tech has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, York Tech is providing notice to the affected residents commencing on April 5, 2024, in substantially the same form as the document attached hereto. York Tech is also offering complimentary credit monitoring to the impacted residents who had their impacted. Additionally York Tech will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. York Tech will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At York Tech, protecting the privacy of personal information is a top priority. York Tech is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. York Tech continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at

Very truly yours,

Spencer S. Pollock

Encl.

York County School of Technology  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998



York County School of Technology  
2179 S Queen St  
York, PA 17402

[REDACTED]

**IMPORTANT INFORMATION  
PLEASE REVIEW CAREFULLY**

April 5, 2024

**RE: Notice of Data Security Incident**

Dear [REDACTED]:

We are writing with important information regarding a recent cyber security incident at York County School of Technology ("York Tech") that may involve your personal information. We wanted to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

York Tech experienced a network security incident that impacted some operations on April 26, 2023.

What We Are Doing.

Upon learning of this issue, we immediately initiated a thorough investigation to determine whether there was any unauthorized access to protected information. The investigative team included external cybersecurity professionals experienced in handling these types of incidents. The extensive forensic investigation and document review concluded on March 15, 2024. It was determined that a limited amount of information stored on our network may have been accessed and/or acquired by an unauthorized individual on or about March 27, 2023. The same unauthorized individual was also responsible for disrupting our operations on April 26, 2023.

What Information Was Involved?

The impacted information includes your

What You Can Do

**We have no evidence that your information has been misused for identity theft or financial fraud.** Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from potential misuse of your information, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with same-day alerts when changes occur to your credit file. The alerts will last for [REDACTED] from the date of enrollment. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [REDACTED] and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

000010102G0500

P

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

*For More Information*

We are committed to maintaining the privacy of personal information in our possession and will continue to take many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

**If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line at 1-833-983-3089.** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

York County School of Technology  
2179 S Queen St  
York, PA 17402

**- OTHER IMPORTANT INFORMATION -**

**1. Obtain and Monitor Your Credit Report**

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. You can obtain a free copy of your credit report by calling **1-877-322-8228**, visiting **www.annualcreditreport.com**, 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/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.



00001020280000

P

***Equifax***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

**2. Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the credit monitoring services, we recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

***Equifax***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

**3. Placing a Security Freeze on Your Credit File.**

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

**Equifax Security Freeze**

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888)-298-0045

**Experian Security Freeze**

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

**TransUnion Security Freeze**

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

#### **4. Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

**Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, <https://www.marylandattorneygeneral.gov/>, Telephone: 888-743-0023.

**New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

**North Carolina Residents:** You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov/](http://www.ncdoj.gov/), Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

**Oregon Residents:** You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392.

**Washington D.C. Residents:** You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.