



RECEIVED

JUL 17 2020

July 10, 2020

CONSUMER PROTECTION
Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Privileged and Confidential

Via Email and Postal Mail

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
DOJ-CPB@doj.nh.gov

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent the McPherson College (“McPherson”), headquartered in McPherson, Kansas with respect to a potential data security incident described in more detail below. McPherson takes the security and privacy of their student and employee information very seriously and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On or about October 3, 2019, McPherson College discovered that a single employee’s email account may have been compromised. McPherson immediately took action to secure the email account and conduct an investigation into the incident. McPherson proceeded to engage a third-party computer forensics firm to conduct a thorough investigation. That investigation concluded in or about November 2019 and found that a single employee’s email account had been compromised. McPherson then proceeded to engage a third-party e-discovery vendor to review the contents of the compromised email account and create a list of individuals that would need to be notified as a result of unknown/unauthorized threat actor accessing the compromised email account. On June 3, 2020, after a thorough and full search of the material accessible within the email account, McPherson received a final list of the names and addresses of the individuals whose information may have been accessed by the unauthorized/unknown third party.

The unknown unauthorized threat actor may have been able to access the affected individual’s name in addition to possibly their Passport number, driver’s license number, government id number, credit card number and CVV, student loan information, limited personal health information, and/or date of birth.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Missouri • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix
San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com



2. Number of New Hampshire residents affected.

A total of two (2) New Hampshire residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on July 10, 2020 by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

McPherson takes the security and privacy of the information very seriously, and has taken steps to prevent a similar event from occurring in the future, as well as to protect the privacy and security of potentially impacted individuals' information. These include but are not limited to implementing multi-factor authentication, forcing password changes, strengthening the security of their email tenant, and reporting the incident to the appropriate government regulators as required. Additionally, the affected individuals were provided with credit monitoring and identity theft restoration services for a period of 1 year through Epiq.

4. Contact information.

McPherson remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

McPherson College (“McPherson”) is writing to inform you of a data security incident that may have resulted in unauthorized access to some of your personal information. We are a private, nonprofit college located in McPherson, Kansas. McPherson is notifying you of this incident as you are either a current student, former student, applicant, or we may have received your information via the ACT or other similar company. While McPherson has no indication that your information has been misused, we are nonetheless providing you with notice of this incident out of an abundance of caution. McPherson takes the privacy and protection of your personal information very seriously. Your trust is a top priority at McPherson, and we deeply regret any inconvenience this may cause you. This letter contains information about what happened, steps McPherson is taking to mitigate the risk of harm, and complimentary resources McPherson is making available to protect you.

On or about October 3, 2019, McPherson College discovered that a single employee’s email account may have been compromised. McPherson immediately took action to secure the email account and conduct an investigation into the incident. McPherson proceeded to engage a third-party computer forensics firm to conduct a thorough investigation. That investigation concluded in or about November 2019 and found that a single employee’s email account had been compromised. McPherson then proceeded to engage a third-party e-discovery vendor to review the contents of the compromised email account and create a list of individuals who would need to be notified as a result of an unknown/unauthorized threat actor accessing the compromised email account. On June 3, 2020, after a thorough and full search of the material accessible within the email account, we received a final list of the names and addresses of the individuals whose information may have been accessed by the unauthorized/unknown third party.

The unknown/unauthorized third party may have been able to access some of your personal information including your name and <<Breached Elements>>.

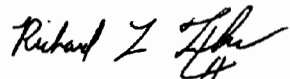
Although we are unaware of any misuse of your or anyone’s information, to help relieve concerns and restore confidence following this incident, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

Additional information describing your services is included with this letter.

We take the security of all information and student records in our control seriously, and are taking steps to help prevent a similar event from occurring in the future. This includes but is not limited to implementing multi-factor authentication, forcing password changes, strengthening the security of our email tenant, and reporting the incident to the appropriate government regulators as required. Please know that the protection and security of your personal information is of our utmost priority.

We sincerely regret any inconvenience that this matter may cause you, and remain dedicated to protecting your information. Please see the addendum for additional steps you can take to protect your personal information. If you have any questions, please call 855-907-2116 Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Richard L. Tuxhorn". The signature is written in a cursive style with a large initial "R" and "T".

Richard L. Tuxhorn, M.Ed.
Vice President for Finance
McPherson College
1600 E. Euclid St.
McPherson, KS 67460
1-800-365-7402

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, marylandattorneygeneral.gov

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov/consumer-frauds/identity-theft>

Colorado Office of the Attorney General Consumer Protection, 1300 Broadway, 9th Floor, Denver, CO 80203, 1-720-508-6000, www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division, 100 W Randolph St., Chicago, IL 60601, 1-800-243-0618, www.illinoisattorneygeneral.gov

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed

below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19016
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.



Activation Code: <<Activation Code>>

Complimentary 12 Month *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

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

- To enroll in this service, go to the *myTrueIdentity* website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Activation Code>> 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 **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Pass Code>> 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 <<Enrollment Deadline>>. 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.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- 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.
- 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. (Policy limitations and exclusions may apply.)