



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

SEP 28 2020

CONSUMER PROTECTION

Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 21, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent the Association of American Colleges and Universities (“AAC&U”) located at 1818 R Street N.W. Washington D.C. 20009, and are writing to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, AAC&U does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 20, 2020 AAC&U was notified by ATS, its IT managed service provider, regarding suspicious activity on a server that hosts AAC&U’s online store software. Upon being made aware of this issue, AAC&U immediately launched an investigation, and began working with ATS to understand the nature and of scope of the incident and what information was potentially impacted by the incident. AAC&U determined that between the dates of April 18, 2020 and May 27, 2020, payment card information entered on AAC&U’s online store was exfiltrated from its environment by an unauthorized actor. The information that could have been subject to unauthorized access includes name, address, payment card number, expiration date, and security code.

Notice to New Hampshire Residents

On or about September 21, 2020, AAC&U provided written notice of this incident to all affected individuals, which includes two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, AAC&U moved quickly to investigate and respond to the incident, assess the security of AAC&U systems, and notify potentially affected individuals. AAC&U installed a patch provided by the software provider to address the vulnerability that allowed the exfiltration to take place. AAC&U is also working to implement additional safeguards and training to its employees. AAC&U is providing access to credit monitoring services for one (1) year, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, AAC&U is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. AAC&U is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,



Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR/eeb
Enclosure

EXHIBIT A



Association of American Colleges and Universities
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

RE: Notice of Data Breach

Dear <<Name 1>>,

The Association of American Colleges and Universities (“AAC&U”) writes to inform you of a recent event that may affect the privacy of some of your personal information. While we are unaware of any actual or attempted misuse of your personal information, we take this incident seriously and are providing you with information about the event and access to resources so that you can better protect your personal information, should you feel it is appropriate to do so.

What Happened? On May 20, 2020, AAC&U was notified by ATS, our IT managed service provider, of suspicious activity on a server that hosts our online store software. Upon being made aware of this issue, we immediately launched an investigation, and began working with ATS to understand the nature and of scope of the incident and what information was potentially impacted by the incident. We determined that between the dates of April 18, 2020 through May 27, 2020, payment card information entered in our online store was taken from our environment. While we are unaware of any evidence of actual misuse of your information as a result of this incident, we are notifying you out of an abundance of caution.

What Information Was Involved? Our investigation determined that at the time of the incident, the potentially accessible information included your name and payment card information.

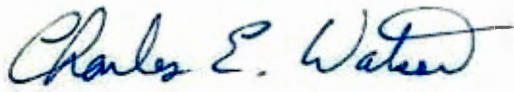
What We Are Doing. The security of information in our care is among our highest priorities. Upon learning of this incident, we quickly took steps to ensure the safety and security of all information held on our systems. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. Although we are unaware of any actual or attempted misuse of your personal information as a result of this event, we arranged to have TransUnion protect your identity for twelve 12 months at no cost to you as an added precaution.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and monitor your credit reports for suspicious activity for the next twelve (12) to twenty-four (24) months. You may also review the information contained in the attached *Steps You Can Take to Protect Your Information*. There you will also find more information on the credit monitoring and identity protection services we are making available to you. While AAC&U will cover the cost of these services, you will need to complete the activation process.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 888-490-0766 between 9:00 a.m. and 9:00 p.m. EST Monday through Friday, excluding major U.S. holidays.

We regret any inconvenience this incident may cause you. AAC&U remains committed to safeguarding information in our care, and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

A handwritten signature in blue ink that reads "Charles E. Watson". The signature is written in a cursive style with a large, sweeping initial "C".

C. Edward Watson, Ph.D.
Chief Information Officer
Association of American of Colleges and Universities

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

As a safeguard, 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.

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 <<Insert Unique 12-letter 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 <<Insert static 6-digit Telephone 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.)

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze on your credit report.

Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

<https://www.transunion.com/fraud-alerts>

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

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 North Carolina residents, you can obtain information from the Attorney General or Federal Trade Commission about preventing identity theft. The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

For Washington, D.C. residents, the Attorney General can be contacted at Office of the Attorney General, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, 202-727-3400, and www.oag.dc.gov.